QUEENSLAND UNIVERSITY OF TECHNOLOGY

Information security management: A case study of an information security culture

by

Salahuddin M. Alfawaz

A thesis submitted in partial fulfillment for the degree of Doctor of Philosophy

in the

FACULTY OF SCIENCE AND TECHNOLOGY

February 2011

Declaration of Authorship

The work contained in this thesis has not been previously submitted to meet requirements for an award at this or any other higher education institution. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made.

Signed: ________________________________

Date: ________________________________

Abstract

This thesis argues that in order to establish a sound information security culture it is necessary to look at organisation's information security systems in a socio-technical context. The motivation for this research stems from the continuing concern of ineffective information security in organisations, leading to potentially significant monetary losses. It is important to address both technical and non-technical aspects when dealing with information security management. Culture has been identified as an underlying determinant of individuals' behaviour and this extends to information security culture, particularly in developing countries. This research investigates information security culture in the Saudi Arabia context.

The theoretical foundation for the study is based on organisational and national culture theories. A conceptual framework for this study was constructed based on Peterson and Smith's (1997) model of national culture. This framework guides the study of national, organisational and technological values and their relationships to the development of information security culture. Further, the study seeks to better understand how these values might affect the development and deployment of an organisation's information security culture.

Drawing on evidence from three exploratory case studies, an emergent conceptual framework was developed from the traditional human behaviour and the social environment perspectives used in social work, This framework contributes to information security management by identifying behaviours related to four modes of information security practice. These modes provide a sound basis that can be used to evaluate individual organisational members' behaviour and the adequacy of existing security measures. The results confirm the plausibility of the four modes of practice.

Furthermore, a final framework was developed by integrating the four modes framework into the research framework. The outcomes of the three case studies demonstrate that some of the national, organisational and technological values have clear impacts on the development and deployment of organisations' information security culture.

This research, by providing an understanding the influence of national, organisational and technological values on individuals' information security behaviour, contributes to building a theory of information security culture development within an organisational context. The research reports on the development of an integrated information security culture model that highlights recommendations for developing an information security culture. The research framework, introduced by this research, is put forward as a robust starting point for further related work in this area.

Acknowledgements

Praise and thanks be to Allah for sustaining and helping me throughout this endeavor. I would like to express my gratitude to the following people for their role in the completion of this thesis:

I would like to express my deep appreciation to my principle supervisor Associate Professor Karen Nelson, for her support, guidance and encouragement over the past few years. I also would like to thank my associate supervisors Dr. Kavoos Mohanak and Dr. Greg Timbrell for their support and recommendations, which improved this thesis. I also would like to thank Dr. Lauren May for her support and help at the start of my study journey.

Acknowledgment is due to the Royal Saudi Air Force for sponsoring my Phd program. I am also very grateful to General Ali Alhamed the Directorate of the Royal Saudi Air Force Commander Office for his support and encouragement that sustained me through this endeavor.

I also would like to thank all the companies and individuals who participated in this research, for being helpful in getting me access to conduct my research, for their help and cooperation; without them I would not have been able to complete my research. Due to confidentiality, I cannot mention their names.

Last but certainly not least, I am forever indebted to my parents, my wife Basimah and my sons Faisal and Mohammed for their endless patience and support.

Thank you all.

Contents

List of Figures

List of Tables

This thesis is dedicated to my family, to my wife Basimah and to my sons Faisal and Mohammed for their time, encouragement and support during the undertaking of my study.

Chapter 1

INTRODUCTION

1.1 Introduction

Public and private organisations face a wide range of information threats. Securing their information has become a crucial function within the information systems management regime. With an increasing reliance on technologies connected over open data networks, effective information security management (ISM) has become a critical success factor for public and private organisations alike. In order to achieve effective ISM, it is essential to develop and deploy an effective information security culture.

Best practice and trends in information security are similar throughout the world. However, when it comes to applying these best practice approaches to specific situations, local context and circumstances need to be considered. This is the case when we consider the application of generic best practices to a specific country, particularly a country which may be considered as still developing technologically, and where there is uneven technological development.

Previous studies have shown that non-technical issues are at least as important as technical issues in safeguarding an organisation's sensitive information (Dhillon and Torkzadeh, 2006; Siponen and Oinas-Kukkonen, 2007). However, the importance of non-technical information security management issues, has been deemphasised in much previous ISM research, which tends to be quantitative in nature (Siponen and Oinas-Kukkonen, 2007). Researchers have also argued that organisations need an information security culture as well as technological mechanisms to ensure a safe environment for information assets (Chia et al., 2002; Ruighaver et al., 2007; Schlienger and Teufel, 2002, 2003; Zakaria and Gani, 2003; Zakaria, 2004). There is a particular lack of attention in the current ISM literature about developing countries and on how factors such as the national and organisational culture, the information security environment and the level of information security awareness, relate to individual attitudes towards information security and its management.

Thus, the challenge is to determine which aspects of an organisation's environment facilitate and enable sustainable information security compliance. This is a complex issue with no easy answers. One aspect that is prominent in the extant literature is that creating a security culture is becoming a key goal for private and public organisations in their attempts to safeguard their information assets. A culture that encourages ethical conduct and commitment to compliance with information security requirements appears to be what organisations need to focus on. In order to achieve this goal, firstly, the environmental factors that influence behaviour and encourage or inhibit individual employees and managers from doing the right thing, even when they know what the policy says, should be identified. Secondly, an effective management strategy that manages internal and external factors should be implemented.

The intent of this study is to contribute to the body of knowledge related to the development and deployment of information security culture in the context of developing countries. Using a case study approach, this thesis examines the factors affecting individuals' beliefs and behaviours related to information security culture. Specifically, the study will examine factors, internal and external to the organisation, which influence information security development and deployment in three different types of organisations (public, private and non-profit) in Saudi Arabia.

1.2 Overview of research problem

The information security discipline is concerned with the quality of information and the technical mechanisms and infrastructures used to protect information assests Information security management focuses on information security governance and ensuring its realisation at the operational level. There are many unresolved problems associated with effective information security management in developing countries.

The current ISM literature seeks to address some of these issues, however, most of this literature adopts a Western culture or industrialised perspective. When the context of information security management is a developing or non-Western or non-industrialised culture, this literature may not be applicable.

This research is concerned with effective information security management in a non-Western culture, specifically Saudi Arabia. The core research problem that this study addresses is:

What organisational elements need to be addressed or managed to develop and deploy an effective information security culture in the Saudi Arabia context?

The motivation for this research is to resolve this problem and thereby provide useful recommendations for organisations' managers and implementers of information security programs in the Saudi Arabia context.

1.3 Research goal

The goal of this research is:

To provide a useful, integrated, practice-oriented and theoretically sound framework that will assist organisations to succeed in the challenging task of implementing and managing quality information security culture within the Saudi Arabia context.

1.4 Research objectives

The objectives of this research study are to:

1. Explicitly identify, present and discuss the information security management practices and cultural factors which may affect implementation and development of information security management in non-Western or non-industrialised cultures.

2. Understand the relevance of each of these identified components, as well as their interactions with each other, and develop from this a holistic framework for developing and deploying an information security culture in the Saudi Arabia context.

3. Assess the resulting framework using data gathered from real-world situations to understand how the component parts of the framework impact on organisation's information security culture development and deployment in the Saudi Arabia context.

1.5 Research questions

In order to achieve the research objectives, the following research questions are constructed:

1) What are the current management practices in relation to information security management and influencing cultural factors in the context of Saudi Arabia?

Information security management literature states that there is a need to address non-technical issues related to security management. Particularly with respect to developing countries, there is a lack of attention in the open literature on factors such as national and organisational culture, environment, and the level of awareness of information security culture and how these factors relate to attitudes towards information security and its management. Hence, appropriate measures need to be designed to protect critical assets.

This question seeks to explore current information security management practices in Saudi Arabia and to identify the cultural factors that influence these practices. Through this question, this study seeks insights into information security decision making and to understand organisational flexibility and adaptability when encountering internal and external information threats, particularly in the context of dynamically changing organizational environments.

2) To what extent do the dimensions of both organisational and national culture influence individuals' related information security practices?

It is well understood from existing literature (House et al., 2004; Schein, 2004; Hall, 1976) that people from different cultures perceive and understand things differently. This notion extends to the domain of information security management. An understanding of the effect of culture on individuals' information security related behaviors may assist the development and deployment of information security management strategy.

In order to establish a deep focus for this research the dimensions of organisational and national culture, will be thoroughly investigated. Through this question, the influence of organisational and national culture on the information security culture and the impact they have on information security management effectiveness will be investigated.

This research question seeks to provide a deeper understanding of the roles of information security management governance and the impact of organizational and national culture. This question will be answered by addressing two investigative questions. The investigative questions are those that the researcher must answer in order to satisfactorily answer the general research question (Emory and Cooper, 1991). This is done by taking the general research question and breaking it down into more specific elements. The investigative questions are:

S-RQ1: To what extent do the relevant values of national culture influence the effectiveness of information security management?

S-RQ2: To what extent do the relevant values of organisational culture influence the effectiveness of information security management?

As these investigative questions are explored and answered in the course of the research, they provide a foundation for the following third research question.

3) How can organisations achieve a quality and successful information security culture with respect to the proposed framework that satisfies requirements of the Saudi Arabia context?

The factors identified are used to develop an information security management model. The resolution of this question seeks to propose a model that will assist in achieving an information security culture in the Saudi Arabia context.

1.6 Research design

This research seeks to better understand the socio-technical elements and processes that impact information security culture formulation and implementation in the Saudi Arabia context. The underlying social and technical dynamics that affect the creation and implementation of information security culture are complex and currently lack definition. Through three in-depth case studies, this research aims to provide a structured analysis of these elements, particularly as they relate to organizational and national values.

This research starts with a literature analysis focusing on key concepts from the areas of information systems management and cultural studies. The initial findings will help to set and refine the study's aims, scope and the research questions. A focused literature analysis about information security management practices is presented to identify possible lessons for enhancing information security management for organisations in the Saudi Arabia context.

An exploratory case study of the information security management practices in the Saudi Arabia context will be conducted that aims to test the extent to which the factors and issues drawn from the open literature apply in the Saudi Arabia context and to investigate other possible cultural and country-specific issues.

The proposed framework and the relationships between the factors in the framework will be applied and verified by collecting data in selected Saudi Arabia organisations using a qualitative approach. These findings will then be related to the information security framework. Figure 1.1 depicts the research design and the steps that will be undertaken during this study:

1. A synthesised literature review capturing information security management factors and values will be conducted.
2. A conceptual framework of information security management factors will be proposed based on the findings of the literature.

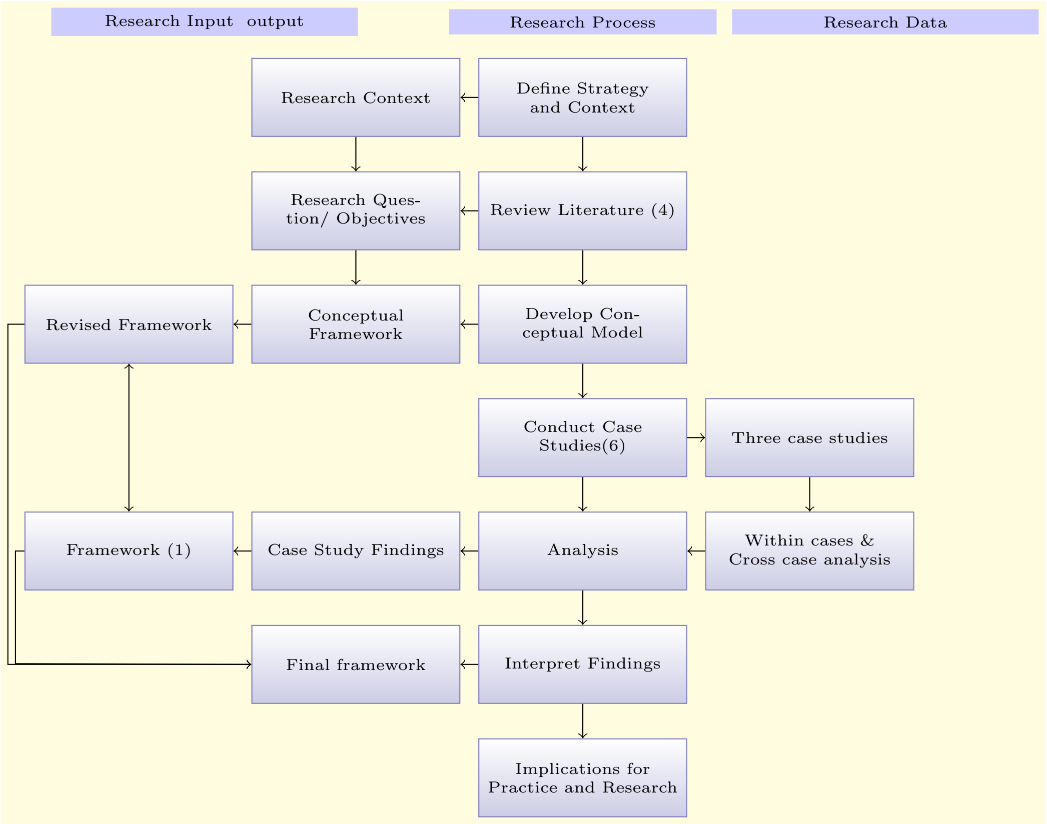


FIGURE 1.1: Research Design

3. Three in-depth exploratory case studies will be conducted to investigate components of the conceptual framework. National and organisational cultural values will be related to information security culture factors and issues. The case studies will be conducted at three Saudi Arabia organisations. There are two aspects to this exploration:

   (a) Documentation about each case organisation will be thoroughly analysed to glean relevant information to determine specific areas needing follow-up in the next phase.

   (b) Semi-structured interviews with members of the selected organisations will be conducted to extend the findings from the documentation and to complete the exploration of the cases.

4. Collected data will be codified and analysed.

5. The findings resulting from the data analysis (4) will then be discussed with respect to the research questions.

6. These findings (5) will then be interpreted within the context of the research framework.

7. The conceptual framework (2) will be refined to reflect the findings arising from (5) and (6)

8. The thesis concludes with a summary of the findings and resulting framework and their implications .

1.7 Benefits of the research

1.7.1 Applied benefits

The outcomes of this research will be relevant to many types of organisations such as government and private for-profit organisations to develop and deploy sound information security cultures to effectively protect their information assets. The applied benefits in this study are:

1. An integrated framework for information security management, which can be used for ISM governance and operations to promote increased awareness of, and consensus towards a workable information security culture.

2. Presentation of a comprehensive analytical model of individuals' information security compliance behaviours.

3. Identification of cultural factors which may impact information security management in the Saudi Arabia context.

4. Provision of examples of information security culture practices that were positively and adversely affected by not taking cultural factors into account.

5. Provision of examples of information security culture outcomes that are associated with information security culture practices.

1.7.2 Academic benefits

The planned academic benefits of this study are to:

1. Identify an appropriate referent theory for information security management related to information security culture
2. Investigate and describe the effects of culture on effective information security management governance and operation.
3. Provide an analysis of information security management activities and information security culture in the Saudi Arabia context.
4. Provide a sound basis for further research into information security management in non-Western cultures.

1.8 Focus of the research

The issues that are considered integral and peripheral to the focus of this research are itemised below.

1. Integral issues: These are the central focus of this research and are investigated in detail.

   a) Activities and factors associated with information security management aspects of information security management programs.

   b) Activities and factors associated with a non-Western culture that may impact upon information security management.

2. Peripheral issues: Although these are not the central focus of this research, reference may be made to them for the sake of completeness. These are not investigated in as much detail as the centrally-focused issues.

   a) Information security roles not related to management of the information security environment.

b) Specific technologies or information systems in relation to the development of information security culture.

c) Specific data or data management systems in relation to the development of information security culture.

1.9 Structure of the thesis

Chapter 1 has introduced the need for a greater understanding of organisational elements associated with effective information security culture in the context of Saudi Arabia. The research questions, study design and potential contributions from the study have been presented. A background to the overall context of the study and the motivations and rationale for the study has also been provided. An outline of each of the remaining chapters follows.

Chapter 2 is the literature analysis. It outlines the foundations of the study. The three main subject areas are reviewed: information security management, information security culture and the cultural dimensions of the Saudi Arabia context.

Chapter 3 presents the initial framework for the research derived from the literature In this chapter, the dimensions of the framework and how they are derived are brought forth. This chapter concludes by presenting the analytical framework used in the research.

Chapter 4 presents the research methodology. A case study method is used. The chapter begins with a theoretical perspective of the research methodology. The background for the selection of the case study method is discussed. Then, the case study protocol including data collection procedures is outlined including their relevance to each phase of the research and how they relate to the research questions. Finally, the data analysis strategy and processes are discussed, followed by a discussion of the issues associated with validity and reliability.

Chapter 5 presents and discusses the research findings that pertain to information security culture effectiveness for each of the three case studies.

Chapter 6 synthesises the findings from the three cases, and refines the conceptual model proposed earlier in Chapter 3.

Chapter 7 concludes the thesis by discussing the outcomes in terms of the research questions and in light of their contributions, significance and limitations. Recommendations for further research are outlined in this chapter.

Figure 1.2 shows the thesis structure.

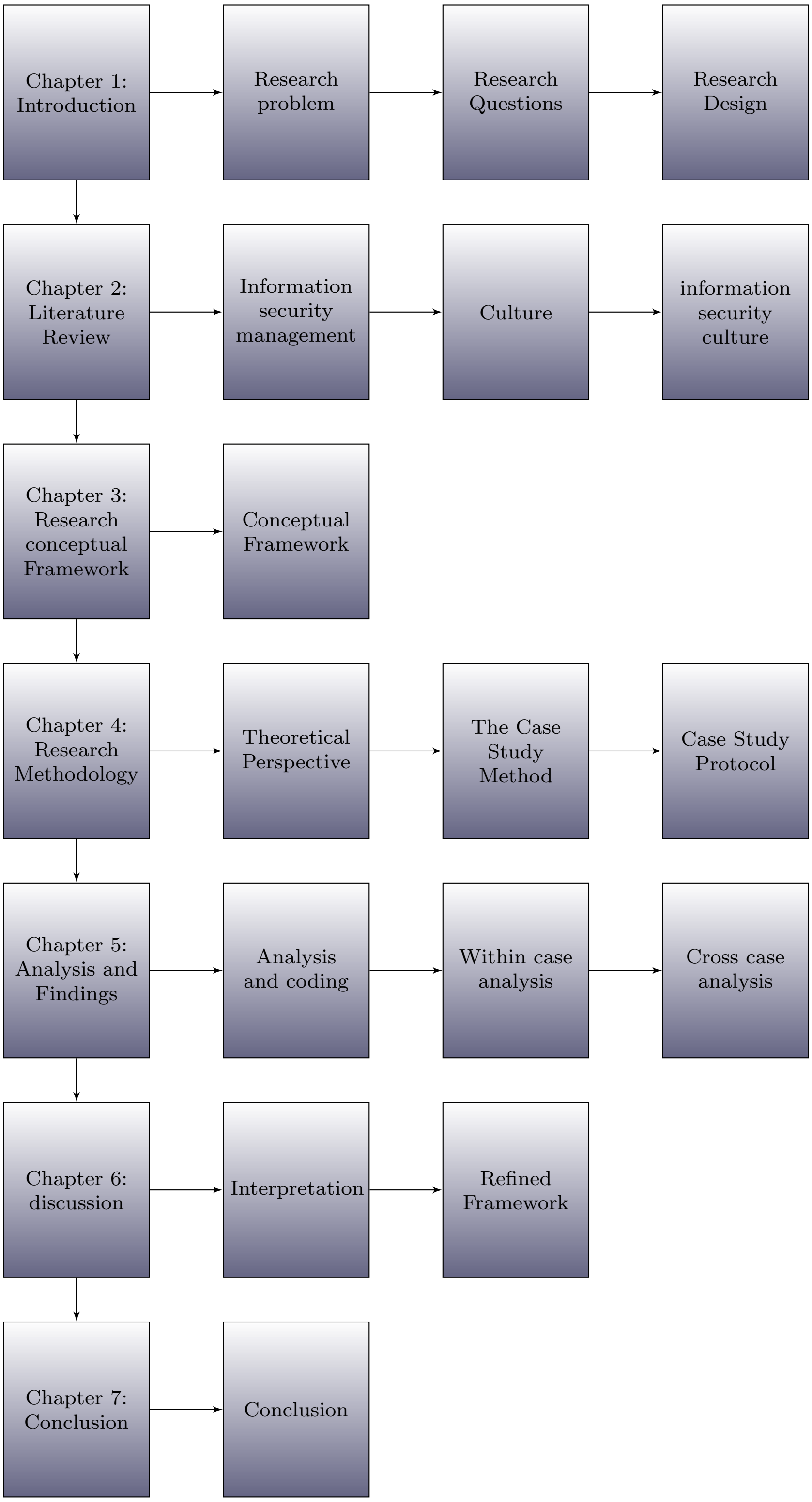


Figure 1.2: Structure of the Thesis

Chapter 2

THE LITERATURE REVIEW

In this chapter, due to the lack of theory and empirical research in information security culture in the current literature, the research review will broadly investigate literature from several perspectives. The current literature on information security management with emphasis on social-technical aspects, and the relevant characteristics of Saudi Arabia were reviewed. The focus will be on factors and issues that have an impact on information security culture development and deployment.

The literature on information security management systems highlights the concept of information security management, in relation to three basic aspects: 1) Information management in the public vs. private sector; 2) Information and knowledge management; and, 3) Country context, and the inter-relationships between these aspects. Also, the role of information security management systems standards and the use of social-technical approaches in addressing these organisational and social issues were reviewed.

The literature reviewed on culture highlights both national and organisational aspects and their relationship with the information systems. The relationship between these two aspects and the information security management system is discussed under the information security culture section.

The reviewed literature on information security culture highlights the problems of information security culture development and implementation, including organisational and social issues.

The review of Saudi Arabia literature highlights the current state of the ICT in Saudi Arabia, the e-government initiative, social and cultural aspects and other related issues.

2.1 Information security management systems

The purpose of an organisation's information system is to provide access to its services anywhere at anytime over closed and open networks. This leads to issues of security and privacy in the management of the information systems. Managing such issues in the public sector has different emphases than in the private sector. The broader information system approach is socio-technical by nature, involving people and processes as well as technologies; hence, particularly in transitional countries, the social culture and characteristics of the country are factors in successful information security management. This means that the concept of information management incorporates three important perspectives of an information system, namely the human dimension, the organisational (public vs. private sector) and the technological dimensions.

The following subsections provide an overview of the current state of these three aspects and how they relate to the concept of information security management.

2.1.1 Information security management concept

Security is traditionally concerned with the information properties of confidentiality, integrity and availability. These properties underpin services such as user authentication, authorisation, accountability and reliability. Other properties such as authenticity, accountability, non-repudiation and reliability are also involved

Waves	Description	Identifying Issues
The Technical Wave Duration: up to about the early 1980s	This wave is mainly characterised by a very technical approach to information security.	Access control lists, user-IDs and passwords.
The Management Wave Duration: from about the early 1980s to the mid-1990s	This wave is characterised by a growing management realisation of, and involvement with, the importance of information security. The Management Wave supplements the Technical Wave.	Information security policies, information security managers and organisational structures for information security.
The Institutional Wave Duration: started in the late 1990s	This wave is characterised by the development of best practices and codes of practice for information security management, international information security certification, cultivating information security as a corporate culture, and dynamic and continuous information security measurement.	Information Security Standardisation, International Information Security Certification Cultivating an information security culture right throughout an organisation. Implementing metrics to continuously and dynamically measure information security aspects in organisations.
The Governance Wave Duration: continues today	This wave is driven by developments in the fields of Corporate Governance and related legal and regulatory areas. It therefore can be described as the process of the explicit inclusion of information security as an integral part of good corporate governance, and the maturing of the concept of information security governance into the business mainstream.	Management and leadership commitment of the board and top management towards good information security; proper organisational structures for enforcing good information security; full user awareness and commitment towards good information security; and necessary policies, procedures, processes, technologies and compliance enforcement mechanisms.

Table 2.1: The ISMS Waves description and issues (adapted from von Solms, 2000; 2006)

[ISO/IEC 17799:2005]. Security mechanisms refer to the technologies that provide the security services; for example digital signatures and firewalls. In this research, information systems security is defined as ensuring business continuity and minimizing business damage by preventing and minimizing the impact of security incidents (von Solms, 1998; Dhillon, 1995).

Much has been published on the changing role of information security (ISO/IEC, 2005; Drucker, 1988; von Solms, 2000, 2006) as the general perception has transformed from the purely technical in the 1970s to its current mainstream role in organisations. From an historical perspective von Solms (2000, 2006) discusses the evolution of information security management systems (ISMS) approaches over the last forty to fifty years by dividing its development into four waves. Table 2.1 provides a brief summary of each wave.

Although this evolutionary concept was developed from the perspective of the technologically developed countries, it is a very useful timeline tool for describing ICT in currently transitioning countries. Each wave describes the general approach to information technology and its management for the given time periods. This concept of a path of ICT evolution can play a significant role in our understanding of the differentiators in ICT technology and the maturity of the information security management system settings in countries which are still in a state of transition somewhere along this path. For instance some countries may not yet have reached the third or fourth wave levels of development. Figure 2.1 visualizes the ISMS waves.

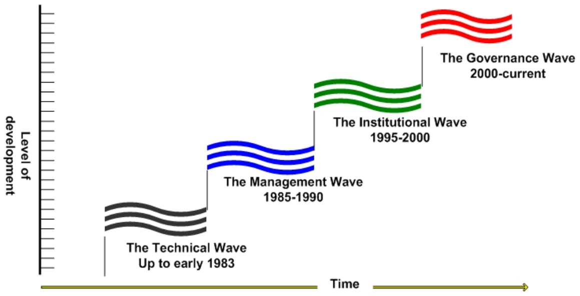


FIGURE 2.1: The waves of the development of the ISMS (von Solms, 2000; 2006)

In the broader sense in contemporary environments, information security involves people and processes as well as technologies. A small number of publications in the literature address the social acceptance of security technologies, referred to as the organisational security culture (Dhillon, 1999; May and Lane, 2006; Ruighaver et al., 2007).

Information security standards are well represented in the relevant literature (von Solms, 1999; Hone and Eloff, 2002; Saint-Germain, 2005; von Solms, 2005). Their usefulness lies more in their character of providing guidelines for application. Sometimes conformance to best practices is assumed to give a competitive advantage and some governmental organisations even require it. In general, these standards have been developed through the experiences of leading technological countries. The role of information security management standards will be investigated more in a following section (section 2.1.5).

The aim of the most recent research on information security management carried out at the micro level (Dhillon, 1999; Siponen and Oinas-Kukkonen, 2007; May and

Lane, 2006; Ruighaver et al., 2007) has been to identify relevant factors of information security management on an organisational basis. Focusing on the internal organisational factors and issues, these micro level studies pay little attention to factors related to the external issues.

Open networks are not inherently secure; therefore attention needs to be paid to aspects of information security within the system itself. It is very important that studies that consider factors of effective information security management relate to both the macro and micro levels as well as guide an understanding of their interrelationships.

2.1.2 Information management in the public vs. private sector

Information management in the public sector is relevant because relationships with external clients of e-government systems need to be carefully managed. Public organisation researchers argue that governments operate in a different environment to private organisations and, hence, require different approaches.

Much has been published in the literature on this topic (Caudle et al., 1991; Newcomer et al., 1991; Fryer et al., 2007; Joia, 2003; Moon, 2000). Several characteristics have been identified. First, the public sector is generally characterised by the absence of economic markets for final product outputs. Second is its reliance on government appropriations for financial resources. This reliance produces another constraint, political influence. specialised forms of accountability may be required that are not typically faced by private sector firms (Bozeman, 1987; Rainey and Steinbauer, 1999; Bretschneider, 1990; Bozeman and Bretschneider, 1986).

Bozeman (1987) distinguished between a public management information system (PMIS) framework and conventional management information systems (MIS) frameworks. He argues that public management information system (PMIS) are likely to emphasise environmental factors more than internal characteristics of the organisation. This indicates that both public and private sectors are likely affected by external factors such as the political authority. However, the public sector seems to be more influenced by those factors than the private sector. Conklin (2007) argues that the differences in these environments play a significant role in the diffusion of technology in e-government settings. It is for this reason that the private sector model can be viewed as inadequate as a basis for management in the public sector (Stewart and Walsh, 1992). Hutton (1996) points out that public sector organisations have a number of specific characteristics, which may have an impact on any change management exercise. Some of these include: rigid hierarchies; organisational culture; changes in policy direction can be sudden and dramatic; overlap of initiatives and wide scope of activities are a crucial part of public sector organisations.

By implication, change management in the public sector is also topical as systems go through development phases (Ward and Elvin, 1999; Ostroff, 2006). Grover et al. (1995) identified the key elements of change management as breaking the organisational status quo and introducing new practices, new values and new structures. In the organisational change concept, the idea is to view the IS development process in terms of organisational change strategies that the developers can effectively use to improve chances of successful IS implementation.

In the current study's context, change management can be defined as managing change in public sector organisations to produce an improvement in the information security management. However, public organisations have been characterised by applying an incremental, slow and only partly top-down change approach, instead of a rapid and complete top-down manner (Hazlett and Hill, 2003; Fryer et al., 2007). While this might be true, the introduction of e-government imposes a strong call for rethinking and reengineering most of the management process in the public sector; for example, stressing the importance of having a senior IT Director/Manager in charge of IT and security programs (Currie, 1996).

2.1.3 Information and knowledge management

Information management (IM) focuses on the “plans and activities that need to be performed to control an organisation’s records” (Place, 1982). Knowledge Management (KM) has become increasingly important and tightly associated with the successful adoption of technology.

Based on knowledge management literature, Bouthillier and Shearer (2002); Nelson (2008), it is argued that IM and KM are complementary, with both required to operate effectively to ensure adequate supply and integration of both ’old and new knowledge’. In particular, knowledge-sharing capabilities are considered key to the success of information security management meeting the needs and demands of organisations’ aims.

There is an inherent tension, however, between the need to secure information and the need to share information. Information security management, at both the governance and operational levels, needs to take this into account. If one considers and accepts that information security is an enabler (as opposed to a blocker), it is recognised that information infrastructures can be developed that cater for the needs of both aspects.

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 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 organisational and individual factors such as organisational culture in support of secure knowledge management systems.

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.

2.1.4 ICT in developing countries

A key aspect in information system management is the country's context, where the phenomenon is deployed and operates. A developing country is generally defined as one that has a per capita gross national product less than US $ 2,000 (Ball and McCulloh, 1990). However this criterion alone is insufficient to describe or denote whether a country can be regarded as "developing" or not. The term "developing" does not imply that all developing countries are experiencing a similar rate or style of development. Each country has its unique setting and constraints such as political and economic ones. Ultimately, these constraints will impose different issues relevant to information security management. It has been suggested that in an environment of low level of democratisation initiatives and low level of ICT readiness, there would be less emphasis on privacy, security, and confidentiality issues (Nour et al., 2007). It is, therefore, necessary to gain an understanding of cultural dimensions that cover both organisational and national culture (Mendonca and Kanungo, 1996; Molla and Ioannis, 2005; Ciganek et al., 2004; Hofstede, 2001) by taking into account the overall context of the developing country in which an organisation operates.

Historically, information security service goals are the preservation of confidentiality, integrity and availability of information. Other characteristics that have evolved from these basics include authenticity, accountability, non-repudiation and reliability [ISO/IEC 17799:2005]. The concepts and principles of information security services and mechanisms remain the same no matter where, geographically, ICT is applied. Given the same degree of foundational preparedness, it is intuitive that there should be no real difference between developing and developed countries in this regard. There is the question, however, of the state of a nation's ICT infrastructure which, for developing countries, may present different challenges and priorities that are worthy of mention.

In terms of information security infrastructure, developing countries in general lack the necessary security technology structures (Aljifri et al., 2003), such as Public-Key Infrastructures (PKI) and adequate encryption systems, to enable a high quality of electronic information. These types of technologies can ensure confidentiality and provide access control, integrity, authentication and non-repudiation services for organisations moving into the information age. This issue is of major concern to many developing countries as it underlies efforts to establish access to the information age through effective ICTs (UN, 2005a).

According to Heeks (2002, 2003) most ICT programs such as e-government in developing countries fail, with 35% being classified as total failures and 50% partial failures. The author attributes these figures to the gap between the current reality (physical, cultural, economic and other contexts) and the design of the ICT program -the greater the gap, the greater the chances of failure. Security has always been identified as one of an information system's important components.

ICT in developing countries is generally under-represented in the open literature. A few publications fleetingly concede that there can be major issues with transitional countries developing their systems, but the subject is not treated in any depth or breadth. The broad existing research on IT in developing countries has recognized different issues and challenges, in particular, the gap between cultures and technology (Heeks, 2002), the lack of skilled manpower (Wiander et al., 2006; UN, 2005b; Bakari et al., 2005; Tarimo, 2006), and the lack of legal development and lack of adequate infrastructure (UN, 2005b; Salman, 2004). Each of these studies provides important insights into a specific issue of ICT initiatives. Most of these studies have addressed the high level issues and focused on conditions rather than actions and behaviours, and on shortages rather than on practical ways of overcoming them. Furthermore, most studies on information security management have paid little or no attention to information security management in developing countries.

Given the widespread perception of IT, particularly e-government, for developing countries, the urgency of their needs, and the frequent paucity of their economic resources, it would be useful to understand in depth the factors and issues that underpin them. While there is some evidence of cultural differences in the ITC adoption, it is still unclear whether these can be related to information security management effectiveness. Yet there are very few published empirical studies directly addressing the issue for some unexplored cultures. This is a main motivation of this research. To narrow this gap, three case studies will be conducted in the current study with the aim to investigate the organisational culture values' and the national culture values' influences on information security culture development.

2.1.5 The role of standards

Adequate information security standards can provide the basis to safeguard an organisation's valuable information (von Solms, 1999). A number of information security management systems standards and guidelines are already in place to address the concept and the requirements for information security management systems. The objective of these standards and guidelines is to protect an organisation's information assets in the context of confidentiality, integrity and availability. In order to achieve the main objectives of this definition, leading technological countries have been working on the development of the necessary information security services and mechanisms for some time. A relatively large number of frameworks, standards and guidelines related to information assurance activities have been developed and published in the open literature. Supporting legislation and regulations have been designed to promote the concepts of information security and privacy on national bases (AS/NZS, 2006; NIST, 2006; OECD, 2002) as well as globally (ISO/IEC, 2005). Another global effort has been made via the IT Governance Institute and Information Systems Audit and Control Association's Control Objectives for Information and Related Technology (COBIT) (COBIT, 2000).

The standards and guidelines provide generic guidance and frameworks, not solutions for the management of information security. They rely on the organisation's risk assessment to determine how they should be implemented and require a policy baseline without providing specifications for compliance with the standard (Hone and Eloff, 2002). Standards and guidelines are mainly driven by the needs of the private sector and lack an authoritative support in terms of which is the recommended one for use in practice. The issues related to the public sector require more consideration, for example, the organisational environment, organisational culture and the diversity of stakeholders. The information security management standards and guidelines predominantly cater for organisations in the developed countries. These standards are generally based upon the availability of certain resources which are generally available in developed countries but need not be sufficiently available in developing jurisdictions. Consequently, certain compromises may need to be made but what these are and how they impact upon risk is still an issue that needs further investigation. For example, Principle (5) in the OECD guideline states that "The security of information systems and networks should be compatible with essential values of a democratic society". This does not necessarily hold true for developing countries. Further standards lack their legitimacy until they are backed with a government decision that enforces the adoption of such standards.

Some public and private organisations have adopted *ad-hoc* solutions or developed their own polices and procedures allowing significant challenges to occur at the integration phase. This diversity has been identified in developed countries as a challenging issue (Lam, 2005), and it would be more challenging in the developing countries. One of the basic challenges encountered in the practical implementation process is the shortage of IT staff that are technically competent in implementing information security standards. Studies (Wiander et al., 2006; UN, 2005b; Bakari et al., 2005; Tarimo, 2006) state that there is a shortage of trained IT staff in developing countries, particularly those who adequately understand and are able to implement information security standards. The information security management standards attempt to describe the various processes and controls needed for successfully implementing an information security policy, rather than advising what the policy should look like (Hone and Eloff, 2002). Also these standards tend to get updated from time to time. This is a challenging issue that organisations need to cope with by applying a mechanism to manage this issue. An information security culture that not is practically addressed by the standards will be highlighted later in a separate section (section 2.3).

2.1.6 The socio-technical perspective

Contemporary information security management recognizes the imperative to include people and processes, as well as the more traditional technology security issues, to ensure the quality of information in contemporary organisations. To a large extent, technological solutions for the majority of security issues have been previously developed. There are, however, still many application challenges, that relate to people and process components of information assurance management. This leads to the need for a socio-technical approach to focus on these issues in the required context for technologically-developing countries. Thus, the human factors represent a key issue that has to be addressed by managers for the information security management effectiveness to take place.

From a theoretical perspective, the organisational aspects of information system security can be categorised into three views: technical, socio-technical and social (Iivari and Hirschheim, 1996). The technical view emphasises that information security development relies primarily on technical aspects. The social view emphasizes the development of organisational systems a head of technical issues. The socio-technical perspective is between these two, viewing technical and organisational systems as equally important.

Goldkuhl and Lyytinen (1982) described information systems as "technical systems with social implications". The concept of the socio-technical approach is built on the assumption that information system development involves the design of a work organisation where its information system has to be compatible with the surrounding social system, that is, the user and the organisational environments (Lyytinen, 1987). This means that a socio-technical model should combine the features of the information system, the user and the organisational environments. It is recognised that technical, organisational and social systems are equally important and that the lack of fit between social and technical systems is the primary cause of information systems problems (Iivari and Hirschheim, 1996).

There are several models of information security in the literature that are based on the concept of the socio-technical approach. The Ives et al. (1980) model of information systems (IS) research is widely known and discussed in the information system management literature. The model distinguishes between three information system environments (user, IS development, and IS operations environments) and three information system processes (use, development, and operations processes). The environments component defines the resources and constraints that dictate the scope and form of information systems and its processes. The Security By Consensus (SBC) model has been suggested by Kowalski (1994), arguing that ICT security can be modeled as an hierarchy of social and technical security measures. Dhillon and Backhouse (2001) proposed the socio-organisational aspects of information security, asserting the need to understand the complex interplay between technological structures and behavioral patterns to ensure proper security.

They aim to address the cultural, social, political and moral aspects of information system security. Dhillon and Backhouse (2001) discuss how socio-technical system approaches can be combined with usability engineering in the design of information systems. Eloff and Eloff (2003) argue that an information security management system (ISMS) consists of many aspects such as policies, standards, guidelines, codes of practice, technology, human issues, legal and ethical issues. It is necessary to identify those human elements that affect the effectiveness of the whole system in order to design strategies that can minimise their weakness. Therefore, when analyzing information security systems, it is necessary to look at organisation information security systems in a socio-technical context.

The three aspects or themes mentioned in Section 1 (information management in the public sector, information and knowledge management and the country context) define the information security management framework within which we explore organisations' security management in developing countries. Such aspects situate the information security management concept within the broader framework of socio-technical theory. For the purpose of this research, the socio-technical view is expected to help in identifying those conditions and human behaviours that have already been found in other social systems and incorporate this knowledge into the analysis of the development of information security culture. The current study focus here is on the effect that culture has on effective information security management. For example, the differences in national culture (non-western versus western) may explain differences in the effectiveness of information security management at the organisational level. Culture has many facets. This research will explore various cultures across both the macro-micro levels and the external-internal viewpoints.

Before moving on to examine the influences of national and organisational culture on security related attitudes, beliefs, and behaviours, it is useful to look at research related to individual information security behaviour and compliance. Dhillon et al. (2007) argues that "computer crime committed by internal employees is essentially a rational act" that could result from internal or external factors (e.g personal factors, work situations and available opportunities). He asserts that behavioural security holds the key for successful information system security management (Dhillon et al., 2007). The theory of reasoned action (TRA) is a theory that seeks to explain an individuals action which is determined by his or her intention to perform a behaviour (Fishbein and Ajzen, 1975). Intention is considered a direct determinant of behaviour in the TRA that is influenced by the attitude (attitude toward performing behaviour) and subjective norms (social pressures to perform behaviour). The forthcoming section will elaborate on information security related behaviour and compliance to better understand these related issues.

2.1.7 Information security behaviour and compliance

Studies have shown that non-technical issues are at least as important as technical issues in safeguarding an organisation's sensitive information (Dhillon and Torkzadeh, 2006; Siponen and Oinas-Kukkonen, 2007). The importance of non-technical issues related to security management, however, is deemphasized in many studies which tend to be quantitative by nature (Siponen and Oinas-Kukkonen, 2007). In particular, there is a resulting lack of attention to the role of the human factor of individual choice and behaviour in the open literature. For example, factors such as the influences of national and organisational culture, environment and level of awareness and how these factors relate to generic attitudes towards information security and its management. Studies have indicated that those factors are seen to be crucial to the success of safeguarding an organisation's assets and that user input is imperative in addressing any information security management strategies or issues (Vroom and von Solms, 2004).

As mentioned earlier the purpose of information systems security is to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents. Information security compromises caused by insiders of the organisation can pose an enormous threat to the organisation's information system. The risk posed to data by insiders (employees and other stakeholders who have physical and/or logical access to organisational assets) should be closely monitored and managed. This risk takes two forms. The first risk is that posed by malicious insiders who deliberately leak sensitive data for personal financial gain or other criminal purposes. The second risk is insiders who unintentionally create data exposures. These can be as a result of their carelessness or attempts to work around security measures. Information security management theorists assert that the behaviour of users needs to be directed and monitored to ensure compliance with security requirements (Vroom and von Solms, 2004; Dhillon et al., 2007; von Solms and von Solms, 2004a). These studies suggest that the success of an information security program depends on the users security related behaviour. Gaining a better understanding of user behaviour characteristics, therefore, can help to assess, improve and audit this behaviour, especially in the nature of security's dynamic changing environments.

The theory of reasoned action (TRA) has extensively been applied as well as its extension, the theory of planned behaviour (TPB)(Ajzen, 1985) in several studies related to information security issues, more specifically in risk perception, and security-related behaviour. Both theories suggest ease of use as an important factor affecting human behaviour. Siponen (2000b) states that the principle of what makes a security solution (e.g.techniques and adherence to procedures) as easy to use as possible has not been addressed in security literature. He suggests that a qualitative research approach would be relevant to address this topic.

Prior research suggests factors that are crucial to security policy adherence and user awareness. For example, Straub et al. (1993) applied the deterrence theory, with the argument that information security actions can deter users from committing unauthorized acts. This also contributes towards improving the quality of policies (von Solms and von Solms, 2004a), promoting security awareness (Straub and Nance, 1990), developing structures of responsibility (Dhillon et al., 2007) and protection by motivation (Workman et al., 2008). Each of these studies provides important insights into a specific issue related to user adherence to security policy. They all refer, to some extent, to the TRA and TPB (Fishbein and Ajzen, 1975; Ajzen, 1985) theories, to understand and test constructs related to individual's security related behaviour.

Most of these studies, however, pay little attention to the fact that attitudes, beliefs, and behaviours of an organisation's employees may be influenced by both national or organisational culture and, more importantly, their interaction. This interaction, in turn, contributes to an individual's beliefs and values towards information security and its management.

The term "*knowing-doing gap*" refers to people who have the knowledge but do not take action or behaviour consistent with that knowledge (Pfeffer and Sutton, 2000). Workman et al. (2008) used this concept to investigate people's security behaviour referring to "people who have been trained but then do not use their new knowledge or skills as management expects". The related literature, however, suggests that an individual user's decision to comply with security requirements is not only a function of the benefit and cost of the behaviour, as described in economic theories, but also, a function of the factors from the users psychology and the social setting the user is involved in.

Three key aspects now need to be discussed. First, although knowledge and skills are very important, they are, however, clearly not enough to assure a positive contribution towards information security culture through the employee's behaviour. Second, a person's set of beliefs, or personal culture, plays a major role in influencing their personal attitude towards their security behaviour (Schlienger and Teufel, 2003). Hence, understanding their underlying beliefs is crucial in the process of behavioural change. Third, the influences of technology, social environment, regulation and self-interest continuously contribute to employee behaviour. As a result some employees and managers could exhibit behaviours of different kinds at different points in time. This continuous movement makes it hard to secure the system by addressing a single mode in isolation.

In light of this, the environmental, in terms of national and organisational cultural values and factors that may influence individual employees and managers' behaviour, are reviewed in the next sections.

2.2 Culture

Culture as defined by Bates and Plog (1976) “is a system of shared beliefs, values, customs, behaviours, and artifacts that the members of a society use to cope with their world and with one another, and that are transmitted from generation to generation through learning”. Hofstede (1984) defines culture as “the collective programming of the mind which distinguishes the members of one human group from another....the interactive aggregate of common characteristics that influence a human groups response to its environment” (p. 25). Culture can also be defined at different levels: at the national, organisational and group level. Hofstede (2001, 1980) asserts that national cultures should be distinguished from organisational cultures. National cultures differ mostly on the values level; while organisational cultures at the levels of practice that are expressed in terms of symbols and rituals. This difference is more fully discussed below.

Culture has been presented as a factor influencing individuals’ performance, adoption of information technology, integration process of information systems, information security management, knowledge transfer and change management. Behaviour is closely related to an individual’s beliefs which are related to their personal culture (Hofstede, 2001; Hall, 1976; Peterson and Smith, 1997). Raman and Wei (1992) concluded that culture had a significant impact on how information technology systems were perceived, used, and adapted.

Studies have indicated that national culture is different from organisational culture because of the different roles played by the manifestations of culture. Culture at the national level is manifest mostly in values and less in practices; culture at the organisational level resides mostly in practices and less in values (Hofstede, 1997). The premise that organisational culture does not develop independently of the national culture in which the organisations operate (Hofstede et al., 1990) puts emphasis on the aspect of the extent to which one level of culture influences the other (Gerhart, 2008). The two possibilities are evident in the literature and among practitioners.

For instance, Hofstede et al. (1990) argue that national culture determines the values of an organisation and its members and that national culture is part of the organisational culture and organisational cultural values reflect those of the national culture. That is, organisational values are strongly influenced by the national culture within which the organisation operates. In contrast, Nelson and Gopalan (2003); Selmer and DeLeon (1996) assert that organisational culture may override the influences of national culture on the values of their members. Straub et al. (2002) seems to hold a middle position between the two views, arguing that different cultures can co-exist and have different salience at different times.

These views coupled with the inherent complexity of organisations suggest that researchers adopt a dynamic approach of cultural interaction in organisational studies. Certainly, understanding cultural values of both levels in combination with other information security systems management antecedents would help to increase the information security culture quality in the organisations. In this research, the focus will be on the national and organisational level and their impact on the effectiveness of the information security management. The proposition of cultural traits of both levels affecting organisational information security culture will be further discussed in the following sections.

2.2.1 National culture

National culture influences how people in certain societies view their duties, interact with each others and express their feelings (Hofstede, 2001, 1993). The role of national culture has been researched in multinational organisations' research. Researchers have investigated how managerial decision making and leadership styles and performance, vary as influenced by national culture. The cultures of developed countries such as Australia, the United States and the United Kingdom are similar. Differences in information security issues between these countries and developing countries such as the Gulf Cooperative Council (GCC) (Saudi Arabia, Bahrain, Kuwait, Qatar UAE and Oman) might be explained by cultural differences (Watson et al., 1997).

The most influential framework of national culture which dominates information systems research is that of Hofstede. Hofstede (2001, 1993) identified four dimensions of national culture: (1) Power distance is the extent to which power is dispersed across the organisation; (2) Uncertainty avoidance is the extent to which the culture feels endangered by unfamiliar happenings; (3) Individualism refers to the degree of importance of an individual's requirements compared with the group's needs as a whole; and (4) Masculinity refers to the extent to which cultures show evidence of masculine or famine qualities. In 1991 Hofstede (Hofstede, 1991) added a fifth dimension 'long/short term orientation', which was an attempt to fit the uncertainty avoidance dimension into the Asian culture. Time orientation refers to the way cultures conform to time by having a long-term time orientation. Guided by the five national culture dimensions, Hofstede analysed a large database of employee values scores collected by IBM company covering more than 70 countries. Hofstede found that differences in national cultures vary substantially along the dimensions of national culture. The variation of country scores along these dimensions shows that different societies have different issues and different ways to adjust to these values.

Some researchers have expressed some concerns about various aspects of Hofstede's dimensions. These concerns have been reviewed (Jones, 2007; Smith, 1992) and addressed by Hofstede (Hofstede, 2001, 2002). For example, using a survey is not an appropriate instrument for accurately determining and measuring cultural values that are culturally sensitive and subjective. Hofstede addresses this criticism stating that surveys are one method, but not the only method that was used. Another criticism is that the data are all derived from the employees of a single company and there are possible dimensions of national culture which did not emerge because they were not presented in Hofsted's questionnaire (Smith, 1992). Hofstede believes additional dimensions should continue to be added to those dimensions.

Although Hofstede's work has been criticised it covers the main dimensions of the national culture (Chapman, 1997; Nakata and Sivakumar., 2001). Hofstede's (1984) dimensions of national culture established and continue to provide the groundwork for many studies that are interested in investigating cultural impacts on different aspects of organisational issues. Three of the five dimensions of national culture that were empirically suggested in Hofstede's studies are theoretically relevant to this study.

Based on several cultural frameworks and data from 825 organisations in 62 countries, the research program team of the Global Leadership and Organisation Behaviour Effectiveness(GLOBE), identified nine dimensions on which national cultures differ. These nine dimensions are: Courage 2. Orientation to the future 3. Sex differentiation 4. Prevention of uncertainty 5. Distance power 6. Individualism / collectivism 7. Collectivism in the group 8. Performance orientation 9.Humanitarian orientation (House et al., 2004). One should note that some of these dimensions present the national culture dimensions of Hofstede's (1980).

Another theorist who has contributed to the dimension of societal culture is Edward Hall with his concept of High vs. Low Context Cultures. Hall (1976) proposed that 'High context' societies prefer implicit communication whereas those in 'low context' cultures are more direct and explicit in their communication. Examples of countries characterised by low context cultures are Australia, the United States and the United Kingdom and countries with High context cultures include the Arab world and Latin America.

According to Hall (1976), in low context cultures, most of the information is contained in the message itself in an explicit and detailed way. On the other hand, in high context culture, less explicit and detailed information is carried in the message itself and inferences are drawn from implicit information. It is accepted that communication is an important facet of information security management (von Solms and von Solms, 2004b; Hone and Eloff, 2002) and effective communication between IT, management and users is challenging enough to achieve in organisations even though the culture is relatively homogeneous. Consequently, in high context cultures, communication tends to be a key issue related to information security. In particular, there is an impact on how information security policy is communicated within the organisation to achieve effective communication. Therefore, this study includes Hall's low and high context dimension.

Peterson and Smith (1997) put forth a model of national culture contributors, characteristics and consequences (see Figure 2.3), which is also relevant to the current study because the model provides us with a comprehensive list of cultural determinants. With this comprehensive list we can examine various issues that are related to information security management besides the country context. Peterson and Smith (1997) use the model to test the relationship between culture and topics of managerial concern. The model proposed ten categories of cultural predictors that are expected to influence people's practices and attitudes. These determinants include language, religion, technology, industry, national boundaries, and climate. Schaffer and Riordan (2003) argues that adding these characteristics to 'country' may enhance the depth of cultural research and researchers can focus on characteristics that are relevant to their specific research context.

The above-mentioned studies clearly indicate that cultural forces of a given society have the power to shape the attitudes of individuals. It is clear that national culture is a crucial factor in organisation studies. Each national culture is characterised by a range of attitudes, values, and beliefs and these are reflected in its members' behaviour. These attitudes, values, and beliefs, to some extent, determine how individuals behave in specific situations and roles. Thus, this research contends that national culture influences the way that information security management is conducted, how information and knowledge would be valued and used, and the overall success of information security management. Therefore, an understanding of these differences in national culture may help managers develop a more effective approach to managing organisational information security systems.

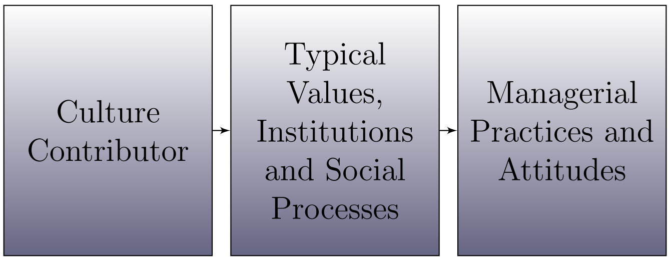

Culture Contributor
Typical Values, Institutions and Social Processes
Managerial Practices and Attitudes

FIGURE 2.2: National culture contributors, characteristics and consequences adopted from Peterson and Smith (1997)

2.2.2 Organisational culture

In general, organisational culture is viewed as a set of assumptions, values, beliefs and practices that would be shared by the entire members of the organisation. Schein (2004) refers to cultures as "the pattern of basic assumptions that a given group has invented, discovered or developed in learning to cope with problems associated with external adaptation and internal integration, and that have worked well enough to be considered valid, and therefore to be taught to new members as the correct way to perceive, think and feel in relation to these problems" . In his early works, Schein attributes the development of the organisational culture solely to the leaders and founders of organisations. Sahin (2004) also argues that leadership qualities are required for establishing a positive organisational culture. According to Schein (2004), organisational culture exists on three levels (see Figure 2.3):

1. Artifacts as seen in organisations are visible, tangible, and audible results of activity grounded in values and assumptions. Artifacts include the behaviour of members of the culture, which is one of the key elements of the present study.

2. Values in organisations are the social principles, philosophies, goals, standards and beliefs considered to have intrinsic worth for members of the organisation. Values include the beliefs held by members of the culture, which are another key element in the present study.

3. Assumptions represent taken-for-granted beliefs about reality and human nature.

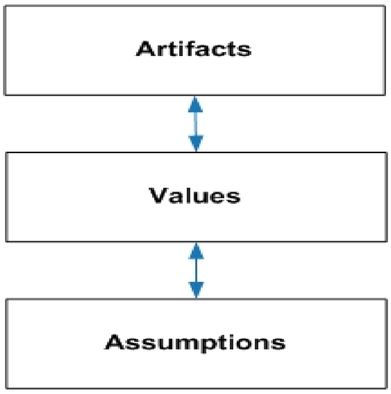


FIGURE 2.3: Scheins (2004) Model of organisational Culture

The importance of the organisational culture as a determinant of success in the introduction of initiatives to manage information security has also been identified (Dhillon and Backhouse, 2001). A key finding of their study was that most information security approaches tend to offer narrow, technically oriented solutions, whilst ignoring the social aspects of security and the informal structure of organisations. They suggest that managing information security requires the adoption of a socio-organisational perspective, of which organisational culture is an integral consideration. However, the values and assumptions of the socio-organisational approach are sometimes narrowly focused on organisational and individual levels, rather than being set in a broader context of values and issues at the national level. Thus, socio-organisational accounts may be criticised for neglecting values and issues at the national level.

2.2.3 The relationship between information systems and culture

The current literature revealed that the impact of culture on information systems management has been extensively researched.

From a national perspective, Poortinga (1992) indicated that national culture places boundaries on human behaviour by defining acceptable and unacceptable behaviours. Based on their empirical work, some authors suggest that cultural values can be used to predict an individuals intention to use an IS and their ultimate acceptance of the system . For instance, Smith et al. (2002) test whether culture-level differences in values can predict the typical sources of guidance on which managers rely in handling a series of what they call work events. The results provide strong evidence that values do predict significant relations found between reliance on a particular source and the frequency of general managers in a nation's sample.

From the organisational perspective, the relationship between information systems and organisational culture was the focus of much research conducted in the information system domain. According to Schein's three level model of organisational culture, behaviours of members of an organisation could be driven by the employees' relevant beliefs (Schein, 2004). Information security, mainly as a particular form of collective behaviour of users and technology occurring in an organisation, has been studied. Based on Schein's model, various studies (e.g. (Schlienger and Teufel, 2002, 2003; Zakaria and Gani, 2003; Vroom and von Solms, 2004; von Solms, 2005; Thomson et al., 2006)) relate elements of information security culture to Schein's three levels of organisational culture. Findings from these studies indicate that organisational culture has a major impact on both information security management and organisational performance.

These studies present a range of different research perspectives. Since all examine the relationship between information systems and culture, much of the analysis is focused on the organisational culture as a system of shared meanings; these levels of analysis tend to predominate, so that the influence of national culture on information security management receives little or no attention.

2.3 Information security culture

Along with the growing interest in the information security culture, there seems to be hesitance and little agreement within the literature as to what information security culture actually is. Chia et al. (2002) state that information security culture does not have a clear definition. Therefore, there are different definitions and perspectives on this topic. Among the definitions of information security culture, we can enumerate the following:

- Dhillon (1995) defines security culture as "the totality of human attributes such as behaviours, attitudes, and values that contribute to the protection of all kinds of information in a given organisation".

- von Solms (2000) calls for the creation of a culture of information security within organisations, "by instilling the aspects of information security to every employee as a natural way of performing his or her daily job".

- Martins and Eloff (2002) describe it as the product of employee behaviour related to information security, which over time ends up being the 'ways things are done around here'.

- Schlienger and Teufel (2002) define information security culture as "all socio-cultural measures that support technical activity methods, so that information security becomes a natural aspect in the daily activity of every employee".

- For Kuusisto et al. (2004) "the unity of values of all parties involved to security culture forming process". They state that if the values of members of the whole organisation are unified, then a unified culture can be formed in less than a few years. However, if the values of members of the whole organisation are not unified, then the process can take significantly longer.

- Ngo et al. (2005) refer to information security culture as "how things are done (i.e. accepted behaviour and actions) by employees and the organisation as a whole, in relation to information security".

Other researchers with definitions along these lines include Kuusisto and Ilvonen (2003), Vroom and von Solms (2004) and Thomson et al. (2006).

In the light of the above definitions, we can infer the way in which information security culture manifests itself within an organisation. Information security culture manifests itself in security related: values, behaviours, attitudes, actions, management related activities and physical environment.

Researchers have applied theories from different perspectives as a basis for information security culture research: from perspectives of an organisational culture perspective (Zakaria, 2004; Chang and Lin, 2007), of organisational behaviour (Vroom and von Solms, 2004), of knowledge management (Thomson et al., 2006), of communication (Schlienger and Teufel, 2002), of change management Ngo et al. (2005), and of total quality management (Chia et al., 2002).

In some studies the information security culture was observed as part of national culture (Chaula et al., 2006) whilst in others there was a specific focus on the culture of the organisation (Schlienger and Teufel, 2002; Vroom and von Solms, 2004; Zakaria, 2004; Chang and Ho, 2006; Chang and Lin, 2007). Results of these studies suggest that organisations must take affirmative steps to create an environment where security is “everyone’s responsibility” and doing the right thing is the norm.

Based on Schein’s model, several studies (e.g. (Schlienger and Teufel, 2002, 2003; Zakaria and Gani, 2003; Vroom and von Solms, 2004; von Solms, 2005; Thomson et al., 2006)) all relate information security culture elements and issues to Schein’s three levels of organisational culture (artifacts, values, assumptions). For example, Zakaria and Gani (2003) gave examples of information security issues related to each of the elements of Schein’s model. These studies suggest that the information security culture is the product of a wide variety of factors which, together, act to influence the degree to which the adoption of a comprehensive management strategy is seen as appropriate. Findings from these studies also indicate that organisational culture has a major impact on both information security management and organisational performance.

In terms of the relationship between the ISM principle of confidentiality and various organisational culture traits, Chang and Lin (2007) found that cooperativeness was negatively related to confidentiality. The characteristics of cooperativeness are cooperation, information sharing, trust, empowerment and team work. The study also found that control oriented cultural traits (effectiveness and consistency) are significantly and positively associated with the ISM principles.

In an attempt to study information security culture, Chia et al. (2002) proposed an information system security culture framework. It was based on Detert et al. (2000), who referred to Hofstede's (1980) national culture dimensions and others. They developed a qualitative comparison along the security culture dimensions of two organisations. Their results indicate differences between the two organisations on several of the dimensions. Their framework covers eight information system security topics that could be used to describe the security culture of an organisation. The information security topics describing information security culture include:

1. The basis of truth and rationale for the belief that security is important.
2. Good balance of long-term and short-term information security goals such as maintaining a secure physical and logical environment and performing security audits several times a year.
3. Security policy and security procedures and processes in place, and security promotion events to motivate employees.
4. Continuous improvement of security, performing of threat and risk assessments.
5. Security has an impact on daily operations of employees.
6. Collaboration and co-operation when developing security policy and managing security.
7. Control, coordination and responsibility of security goals are well defined.
8. Security requirements conform to external audit and governmental requirements.

Chia et al. (2002) argue that increasing the participation levels of employees in security decisions will lead to the belief that security is of the utmost importance. In a subsequent study, Ruighaver et al. (2007) chose a single dimension of Chia et al.'s (2002) security culture framework aspects(control, coordination and responsibility), to link security governance to security culture. Their aim was to explore how security governance can influence information security culture. They found that social participation is a key component in security governance that may influence the levels of responsibility. They suggested that social participation needs to be formalized into the organisational structure.

The national culture aspect, however, is not clearly presented in the information security topics identified by Chia et al. As mentioned earlier cultural dimensions (power distance, uncertainty avoidance, individualism, masculinity and time orientation) are presented in the context of Hofstede's (2001) national culture dimensions. Studies suggest that developing countries encounter both organisational and national cultural obstacles when attempting to transfer technology, created abroad, into practice at home (Yavas, 1992). Straub et al. (2002) proposed a social identity theory to be used as a grounding for cultural research in information systems. Social identity theory suggests that each individual is influenced by different level of cultures. This means that considering only the organisational culture is not enough for understanding the influencing factors on information security culture.

Macro and micro perspective approaches to information security management factors will be used in this research. The macro level endpoint concerns the country context and the global environment, while the micro level endpoint concerns individual practices and personal incentives. Organisational and other levels perspectives fall somewhere within the range defined by these two endpoints.

The macro and micro terms have been used by a number of researchers to analyse different applications and issues related to the information management discipline. For example, drawing on Markus and Robey (1988), Dibbern et al. (2004) used this perspective to analyse the theoretical foundations used to study information system outsourcing. Mohannak and Hutchings (2007) propose a cross-cultural and institutional framework for understanding the effects of culture on knowledge management styles. They argue that such a framework should include at least three dimensions: contextual factors (macro), the participants (micro), and the KM process (organisational). Von Solms (2000) argued that information security must be managed on both a macro and a micro level. The macro level (information security at an inter-organisational level) should be managed with the help of, and measured against, an internationally accepted framework such as the 27002 standard. The micro level (information security at the intra-organisational level) should be managed through a dynamic measurement system.

It is not conclusive that cultural traits such as (power distance) and traditional values can affect decision making and employee involvement in developing countries or hinder the effectiveness of information security programs there. Kanungo and Jaeger (1990) argued that the socio-cultural environment of the developing countries, when compared to the developed countries, is relatively high on uncertainty avoidance and power distance, and relatively low on individualism and masculinity. In terms of information security management, these values may tend to reinforce resistance to ICT among developing countries and, consequently, contribute to a lack of compliance to relevant measures or controls that would be implemented to safeguard an organisation's information assets. Recht and Wilderom (1998) state that the transfer of Enterprise Resource Planning (ERP) into developing countries is likely to face the "double-layered (national and organisational) acculturation" impact. Hence, it is essential to address cultural dimensions that cover both national and organisational aspects.

The argument over whether information security culture can be measured, managed and manipulated have been addressed in the literature (see for e.g. (Schlienger and Teufel, 2003; Chang and Lin, 2007)). Schlienger and Teufel (2003) state that information security culture can be analysed and measured through "the measurement of the artifacts: management and work processes, use of methods, design of physical things, rituals, symbols etc". They argue that these measurements of the artifacts are easier to analyse and measure. According to Chang and Lin

(2007) the culture of an organisation can be built or changed by important factors of culture, such as norms, beliefs, values, and expectations. In this research, the assumption is that information security culture can be measured, managed and manipulated. At the same time, information security culture, is difficult to change, as that assessment and willingness must be achieved among actors within the organisation.

The information security culture literature shows that most of the current studies are focused on policies and awareness creation, but few studies have addressed the development and creation of the information security culture process (Vroom and von Solms, 2004; Ngo et al., 2005). Vroom and von Solms (2004) proposed that security culture can be cultivated by management, learned and reinforced by employees and passed on to new employees. They argued that cultivation of security culture is possible through Nonaka's modes of knowledge creation between tacit and explicit knowledge. Ngo et al. (2005) maintain that identifying the key roles of management and employees in these three phases is crucial for successful organisational information security culture change. They suggest that a successful transition to information security culture environment requires the completion of three phases: (1) ending; (2) neutral zone; and (3) new Beginning.

The research work presented in Sections 2.3 and 2.4 constitute a different attempt to understand the concept of information security culture. These studies argue that in order to institutionalize proper user behaviour towards information security within an organisation, a security culture has to be created. In general, these studies refer, to a greater or lesser extent, to Schein's model, to test constructs such as individuals security related behaviour and effective information security management. The dimension of national culture, however, has had little attention or has been neglected in terms of information security culture. Few information security culture researchers acknowledge the possibility of multiple cultures existing within one organisation (Kuusisto and Ilvonen, 2003; Ramachandran et al., 2008). This indicates that information security culture involves different actors, holding sometimes contradictory values and assumptions. Table 2.2 presents a summary of recent information security culture related literature. The manifestations of information security culture can be represented as in Figure 2.4.

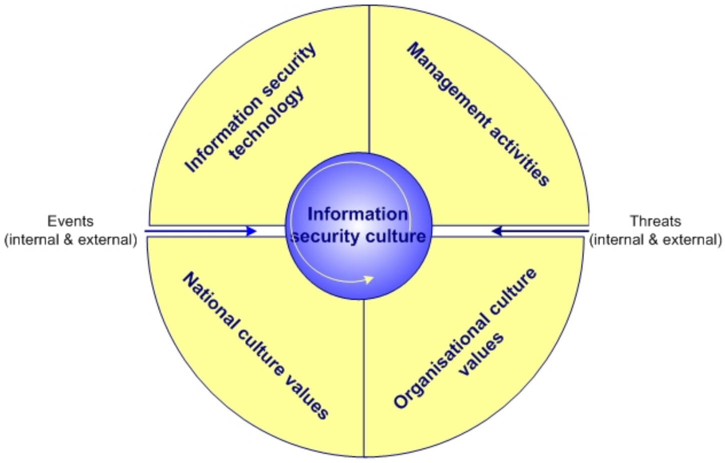

Information security technology
Management activities
Events (internal & external)
Information security culture
Threats (internal & external)
National culture values
Organisational culture values

FIGURE 2.4: Information Security culture

Further, most of these studies tend to neglect the shifting view of culture, as not being static but rather, as an ongoing process (Walsham, 2002). As threats increasingly evolve and the rate of technology changes more rapidly then the context within which that organisation operates will become more vulnerable to various threats. The introduction or change of new technologies and business practices may lead to integrations and transformations between various aspects of information related values, assumptions and behaviour. An organisation that fails to maintain an effective information security management in this dynamic environment will find itself increasingly subject to severe threats from inside and outside. It is important, therefore, to understand internal and external events and issues that could lead to any threats to compromise the quality of the information security culture. These forces (events and threats) have been depicted in Figure 2.6 to reflect the view of information security as an ongoing process, each of which will be reviewed more using representative literature in Chapter 3.

Table 2.2: A summary of current research of information security culture

Study	Findings/Conclusions/Constructs
(Koh et al., 2005) (Ruighaver et al., 2007)	Formalisation of social participation to influence the levels of responsibility
(Kuusisto et al., 2004)	A unified culture of security must be communicated to customers and other organisations.
(Schlienger and Teufel, 2002) (Chia et al., 2002)	Increasing users' involvement and participation in security decisions.
(von Solms, 2000)	Changing of awareness programs into continuous organisation information security plans.
(Ramachandran et al., 2008; Kuusisto and Ilvonen, 2003)	Attention should be paid to differences in security cultures within one organisation and across professions.
(Van Niekerk and von Solms, 2006)	Security knowledge could be a fourth layer to Scheins model orgnizational culture.
(Ngo et al., 2005)	Identifying roles of management and employees in the transition process.
(Zakaria et al., 2007)	Embedding management activities in information security.

2.4 The case study (Saudi Arabia)

Saudi Arabia has been undergoing rapid, major change in all aspects of social, political and economic life. In the past few years of the transformation, the changes included the introduction of a mass privatisation program and the establishment of new institutions supporting the knowledge-based economies, as well as the introduction of related laws. As a result of numerous economic and political reforms, Saudi Arabia was able to achieve an advanced position in the knowledge-based economies. This relative economic and political success would appear to indicate that these initiatives have been to a significant extent efficient. However, given the demands of the knowledge economy, Saudi Arabia is faced with the need to effectively manage these initiatives at all levels. Clearly, there are still significant challenges ahead for Saudi Arabia's organisations, especially in the area of information security management. In this regard, there is little research about information security management and its issues in Saudi Arabia. In fact, an extensive search by the author of large databases and libraries did not return any research that was entirely dedicated to information security management and related issues. The materials and information used in this section were drawn from different studies on various related topics.

2.4.1 ICT in Saudi Arabia

The Gulf Cooperation Council (GCC) comprises of Saudi Arabia, Bahrain, Kuwait, Oman, Qatar, and the United Arab Emirates. GCC is a regional organisation involving the six Arab Gulf countries, with common economic and social objectives in mind. Recently, the GCC countries have made great progress in moving into ICT knowledge-based economies. The governments have been the prime investigators in the advancement of information technology. They have funded significant projects in IT related industries. The rapid growth in IT is evident from the countries' improvement in the position of e-government ranking, e-readiness ranking and networked readiness index ranking (UN, 2005b)and (UN, 2005a).

Saudi Arabia is the largest country among the GCC countries, with nearly 60% of the total population. The Saudi Arabia National Five Years Plan for Information Technology sets the country's vision for bridging the technological gap between Saudi Arabia and the developed world by 2020 (CITC, 2006). The Internet and broadband were introduced in Saudi Arabia in early 1999 and 2001 respectively. Based on 2006 statistics, the Communications and Information Technology Commission (CITC, 2006) reported that Internet penetration is rapidly growing in Saudi Arabia, with a rate of around 19.6% annual growth. Broadband uptake is increasing at a rate of 1% per annum. This is compared to the world and developing countries which average 5% and 20% per annum increases respectively.

The CITC developed two draft laws, the e-Transaction Act and the e-Crime Act. Both were approved and issued in early 2007. The National Centre for Information Security was established in 2006, which has been called the Saudi Arabian - Computer Emergency Response Team (CERT-SA). The centre is expected to play an important role in cultivating awareness, management, detection, prevention, coordination and response to information security incidents at the national level (CITC, 2006).

Although these initiatives are highly regarded, much work still needs to be achieved with respect to information security management. Abu-Musa (2007) conducted a study to evaluate security control in Saudi Arabia. The author found that 50% of the responding organisations had had a significant financial loss as a result of internal and external security breaches. The study also found that, as a result of low levels of security awareness and other reasons, employees conducted activities such as: deliberate and accidental entry of bad data; sharing of passwords; introduction of computer viruses; suppression and destruction of output; unauthorized document visibility; and directing prints and distributed information to people who are not entitled to receive them.

2.4.2 Saudi Arabia e-government initiative

The strategic vision of the Saudi Arabia Ministry of Finance and National Economy is based on a decentralised approach in executing e-government projects (CITC, 2006). These projects are divided into two types. The first type are projects related to the activities of a ministry or a government agency, in which case the ministry or agency is responsible for executing the project according to a set of rules and regulations. The second type are joint projects benefiting several ministries, as forming part of the infrastructure for e-government. In the latter case execution is the responsibility of the e-government program.

Saudi Arabia scores 0.4105 on the United Nations e-government readiness index (UN, 2005b). This is almost at the world average score, which stood at 0.4267 in 2005. In technological terms a key indicator for e-government readiness is the extent of Internet access. Saudi Arabia has much potential and need for the development of e-government services and applications.

The following subsection provides a summary of the relevant literature on the social and cultural aspects of the Saudi Arabia context.

2.4.3 Social and cultural aspects

This section seeks to provide as much of an understanding of the Saudi Arabia culture at the national and organisational level as is possible including brief description of Saudi Arabia's major traditional values and cultural traits. To some extent, the investigation provides a picture of the culture of the Saudi Arabia people and nation in a broad view. It seeks to cover the most significant and representative traits and features that are deemed likely to exert an impact on information security management.

The current literature views Saudi Arabia IT management and culture from within the Arab region. Relatively, the culture of Saudi Arabia can be described as more of a homogeneous culture. The Islam religion and Arabic culture have long been the predominant features of Saudi Arabia society and continue to manifest themselves today in many aspects of daily life, especially in human relations and organisational activities. Some of these values and features include: family-orientation, morality and ethics, tribal system and collectivism versus individualism. Saudi Arabia's political structure is a product of its predominant traditional and centralised monarchic government system. The government has the responsibility for major public services. Saudi Arabia is guided by the Islamic Law *(Shari'ah)* and the institution of Shura. This carries with it the many socio-cultural and economic implications that Islamic values may have in affecting human relations and organisational activities (Choudhury and Al-Sakran, 2001).

This scheme to some extent helps to explain the society's views on certain values and the functioning of the governing mechanism. For example, Islam and Arabic values highly value emotional ties and attachment to relatives and community as well as help extended to each other. In this way, they foster the sense of collectivism. The tribal system plays an important role in the work place. For example, individuals may sometimes give preference to their relatives while discharging their responsibilities even though this act is against their workplace ethics.

It could be stated that Saudi Arabia organisational behaviour, to some extent, is a reflection of the country's culture at all different levels, demonstrating Islamic and Arabic values. To illustrate this more, Saudi Arabia national culture can be characterised using Hofstede's national culture dimension framework.

According to Hofstede's national culture index scores (see Table 2.3), the Saudi Arabia national culture is more accepting of social inequality and uneven power distribution within organisations compared to the western national culture. The Saudi Arabia organisational culture is more likely to be hierarchical and pyramidal in nature, contrasting with its western counterparts that emphasise equal opportunity and flat organisational structure.

According to the index, Saudi Arabia is a collectivist society. The Islamic religion and Arabic culture all emphasise strongly family values and bonds with relatives. Within a company, collectivist cultures would prioritise the good of the company

TABLE 2.3: National culture values across cultures- Adopted from Hofstede (1980)

Culture values	**Arab countries (including Saudi Arabia)**	**Australia**	**USA**
National culture Hofstede (2001)			
Power distance	High	Low	Low
Uncertainty avoidance	High	Low	Low
Individualism vs Collectivism	Low - High	High - Low	High - Low
Context: Hall (1976)	High	Low	Low

before the good of each individual. Saudi Arabia is intolerant towards uncertainty and ambiguity in work-related situations. The higher score for the Arab world on this dimension suggests that Saudi Arabia is intolerant of unusual ideas and behaviours and has a high respect for authority (Hofstede, 1984). People in such cultures are hardworking, obedient (Rawwas, 2001) and tend to yield to the directives held by superiors, who establish rules and long-range plans that can shield them against anxieties about the future.

As mentioned earlier, Islamic religion and Arabic cultural values exist concurrently, influencing people's perception and behaviour in different ways. Al-Jafary et al. (1989) conducted a study of managers in Saudi Arabia in relation to leadership styles. The findings indicated that the economic environment and the cultural and religious orientations of managers in Saudi Arabia significantly influenced their scores on Machiavellianism and the relationships between their needs and leadership styles. In comparison to the U.S. norms, the Saudi Arabian managers were found to be lower on Machiavellianism. Reimers and Barbuto (2002) argue that those scoring low on a Machiavellian assessment would be less likely to strategically alter their behaviour. In terms of information security, one may infer that managers in Saudi Arabia organisations are likely to exhibit resistance to new rules and procedures.

Bjerke and Al-Meer (1993) also analysed Saudi culture along the four cultural dimensions defined by Hofstede (1984), concluding that Saudi managers scored high on power distance, relatively high in uncertainty avoidance and high on collectivism and femininity. They attributed Saudi managers' high scores for collectivism to Islamic values. However, these researchers based their conclusions on data from Saudi MBA students and their co-workers. This data may not be representative of Saudi managers as a whole.

Straub et al. (2001) proposed a cultural influence model and suggested that Arab cultural beliefs were a strong predictor of resistance to IT transfer. The same model has been applied (Loch et al., 2003) to examine culture-specific enablers for the adoption and use of the Internet in the Arab world. The findings of this study indicate that social norms can impact the individual and organisational acceptance and use of the Internet in the Arab countries. In a recent study, Al-Gahtania et al. (2007) applied the unified theory of acceptance and use of technology (UTAUT) model in Saudi Arabia in determining 'intention to use' and 'usage behaviour'. They state that the low individualism country score for Saudi Arabia might indicate a strong relationship between subjective norms and behavioural intentions in the Arab world. This indicates that Saudi users' subjective norms positively influences their intention.

Hunt and Attwaijri (1996) indicate that Saudi executives' values are derived mainly from Islam and show a moderate tendency towards individualism. They state also that Saudi executives give their friendships and personal concerns more importance than the goals and performance of their organisation. However, these authors did not specify whether these priorities are expressed conceptually or practically (Smith et al., 2007).

It could be stated that the new generation of managers in Saudi Arabia are generally more open to new ideas and willing to take risks. Of course, this tendency can be traced to the strong influence of the presence of western companies and expertise in Saudi Arabia. To some extent, this tendency is reflected in a greater tendency to take risks in business by managers in Saudi Arabia's organisations.

The existing literature thus provides only a partial view of Saudi Arabia IT management and culture from within the Arab region. There is a lack of systematic descriptions of the behaviour of Saudi Arabia managers and users. The prevalence of Islamic and Arabic values through the region has led many researchers to generalise about shared aspects of Arab culture. However, there is a need to consider the extent to which the distinctive political, economic and IT development experiences of Saudi Arabia may have influenced the information security related behaviours and attitudes of organisations and their members.

2.5 Summary

The purpose of this review is to look at the fields of information security, information management in the public sector, culture and information security culture and concepts and issues related to information security management. Existing literature and past studies were analysed with the intent of investigating information on different aspects of information security management. It also necessitated exploring tools applied by other researchers to assess the environment of information security culture. All this was to be looked at in the context of other works that studied the relationship between national and organisational culture and managerial aspects of an organisation in general and information security culture in particular.

Literature analysis has revealed that security is one of the main ingredients in the success or failure of any information system. Current research in information security related to the public sector shows that non-technical issues are critical for the organisational change process, and that therefore, more attention should be given to those issues. There are many different standards, guidelines and relevant models have been presented to suggest solutions for these information security issues. The majority of ICT management standards and best practice guidelines have been developed by technologically advanced countries. The management of information security culture is a relatively recent focus with which even technologically advanced countries have unresolved issues. Those standards are considered by many researchers as generic guidelines not solutions; consequently, addressing the specific issues of developing countries with respect to their management of information security issues is outside the scope of these standards.

For countries which are still developing technologically e-government security management has added issues, mostly to do with environmental factors which differentiate them from the implicit assumptions of more technologically advanced countries. The main research question is whether or not the management of information security for developing countries is fundamentally different from that in technologically advanced countries. Initial indications are that, although the technology itself is essentially the same globally, environmental factors influence its application and, hence, impact on the resulting degrees of success of information security culture development and deployment.

Culture can influence information security in many ways. In the real setting, an employee's behaviour is based on values, beliefs and knowledge about information security requirements. This is gained from both social dimensions (e.g. national and organisational culture values) and management activities (through advertising such as training , awareness and empowerment system). Based on these factors an employee processes the information and then makes decisions. Thus, the link between national culture and information security culture is primarily a link between values and behaviours of an organisation's employees. Researchers have quite frequently tested culture-level associations between value dimensions and behaviours from two perspectives: national and organisational. However, the influence of national culture on the effectiveness of information security management has not been extensively researched.

The existing literature on Saudi Arabia provided only a partial view of Saudi Arabia IT management and culture from within the Arab region. There is a lack of systematic descriptions of the behaviour of Saudi Arabia managers and users, particularly, those related to information security management.

Current research in information security related to information security culture development shows that there is still a lack of empirical studies in the current literature about the information security culture concept. Research also shows that there is an increasing need for comprehensive but specific approaches to information security aspects that would assist management in developing and deploying information security culture in the context of developing countries. Furthermore, the existing frameworks for information security culture are inadequate because they do not incorporate the country's specific factors satisfactorily. In addition, most of these frameworks lack empirical evidence and being limited to few factors to be adopted for investigating a complex phenomenon in the context of developing countries. However, the work developed in later chapters will build on the techniques and strategies introduced in these frameworks.

In general, this review has demonstrated that there is still much to be developed in the field of information security culture concepts and practices. Therefore, what developing countries, such as Saudi Arabia, require are methods or techniques that can help them reduce costs associated with information security risks while at the same time taking advantage of the new technology and considering the country's specific features. Information from this chapter will be used to develop the research framework in Chapter 3 and research methodology in Chapter 4. The next chapter will discuss a proposed framework that takes socio-technical issues and the country's features into account to develop or improve an organisation's information security culture .

Chapter 3

THE RESEARCH FRAMEWORK

In this chapter, a preliminary framework is proposed conceptualising the main dimensions for information security culture in the context of developing countries. The proposed framework will serve as a guide to the data collection process including the choice of interview research questions, which are detailed in Chapter 4. The framework will then be updated and refined further as data is collected and analysed. The revised model will be presented in detail in Chapter 6.

This chapter expands on the following issues. First, the theoretical foundation underlying the conceptual framework is highlighted. Second, the premises underlying the framework are elaborated and the key terms used in the framework are explained. Third, the framework is developed and the theoretical and/or empirical underpinnings of each relationship are discussed. Finally, concluding remarks on the proposed framework are presented.

3.1 Research conceptual framework

The literature on the three aspects of information security management, IT management in the public vs. private sector, and the country context, considered in this thesis, has suggested several values and factors that may influence the success of information security culture development. The investigation of these values and factors in the context of developing countries forms the basis for this research.

Information security as a particular form of collective behaviour of users and technology occurring in organisations has been mainly studied from the technical perspective. However, recent studies (e.g. Dhillon and Torkzadeh 2006, Dhillon, 2007 and Siponen,2007) show information security effectiveness is not only a function of the effectiveness of the technical requirements but also a function of the factors and values such as the managerial efforts, the users psychology and the social setting the user is involved in. Yet, these factors and values in information security management have received very little attention.

As discussed earlier, the final objective of the empirical investigation in this study is the development of an appropriate generic model for information security culture development and deployment in the context of Saudi Arabia.

It has been suggested (Miles and Huberman, 1994) that researchers use a predefined structure to set out their expectations while remaining flexible to unanticipated outcomes. This structure, referred to as the conceptual framework, is based on existing theoretical and empirical knowledge. Miles and Huberman (1994) indicate that the conceptual framework ”explains, either graphically or in narrative form, the main things to be studied, the key factors, constructs or variables, and the presumed relationships between them”.

In order to study the information security culture which is required for an effective information security management, a pre-defined framework is proposed.

From a theoretical perspective this study is a contextual analysis, as the intention is to find and understand linkages between: behaviours, attitudes towards values, factors and issues associated with information security, knowledge sharing and change management, to assess the overall state of an organisation’s information security culture.

Frameworks such as the theoretical perspective of national culture (Hofstede, 2001; Hall, 1976), organisational culture (Schein, 1985), the individual level theory of reasoned action (TRA) (Fishbein and Ajzen, 1975) and the Theory of planned behavior (TPB) (Ajzen, 1985) suggest that there is a strong relationship between values, beliefs and people's behaviour. In this sense, we assume that the information security behaviour is influenced by attitudes and values inside and outside the organisation. Thus, the link between national and organisational culture and information security culture is primarily manifested in the relationships between values and behaviours of an organisation's employees.

Peterson and Smith (1997) proposed a model (discussed in Section 2.3.1) of national culture contributors, characteristics and consequences. The model suggests ten categories of culture predictors that are expected to influence people's practices and attitudes. For the purposes of this research, we elaborate on this model and include the outcome of an organisation's managerial and employee practices.

In determining what attributes to examine in this research, the present study relies primarily on the extensive work of Hofstede (2001), Hall (1976) and Chia et al. (2002). The study chooses to draw from those frameworks because they cover both the organisational culture dimensions and the national culture dimensions. This is to include macro and micro factors that may affect information security culture values and practices in the Saudi Arabia context.

These aspects are limited to those values and beliefs that are expected to have an influence on the information security culture development and deployment and are specific to the culture being studied. The current study focuses on understanding the organisation's perspective about the following: information security management, information and knowledge sharing and change management factors and issues.

3.2 The conceptual framework premises

The current study is built on three premises. Support for each premise from literature has been highlighted in the literature review in Chapter 2.

First, we assume, in this research, two types of contributors can influence an employee's security behaviour to choose an option (whether choosing to comply with the information security procedures and rules or not). The first type is the internal environment contributors (e.g. organisational culture). The second is the external environment contributors (e.g. national culture).

Second, in developing countries, the double-layered (national and organisational) impact is likely to influence employees' security behaviour. Hence, it is essential to address cultural values that cover both national and organisational aspects.

Third, information security culture can be managed and manipulated. At the same time, security culture is difficult to change and actors within the culture must participate in the change process. Thus, the changes associated with information security technology, threats and business changes constitute an ongoing process rather than a static one. Figure 5.1 depicts these components and their interrelationship.

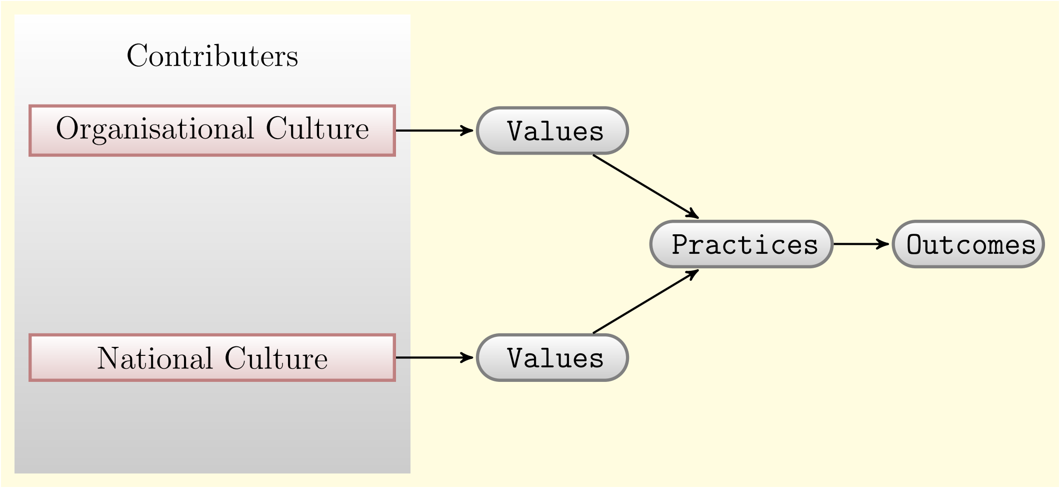


FIGURE 3.1: Research Conceptual Framework

3.3 The conceptual framework aspects

This research adopts the following concepts in the conceptual framework that is being proposed:

Organisational culture dimension: represents the relevant values and beliefs structure of the organisational culture in a given organisation. This is conceptualised by the managerial security activities which organisations can perform to either optimise their information security culture or adapt them to emphasise and achieve information security culture through appropriate management and employee behaviours. Examples of the managerial security activities are: security related standards, policies, procedures, security training programs, and security awareness programs.

National culture dimension: represents the relevant values and beliefs of the national culture in a given country. This is conceptualised by the four national cultural values of (Hofstede, 2001) (Power distance, Uncertainty avoidance, Individualism vs. Collectivism) and Context (Hall, 1976), which are believed to have influence on the security-related behaviours of an organisation's employees.

Information security practices: represent the security-related behaviour of an organisation's employees that is influenced by values relevant to the technological, national,and organisational culture aspects. For example, compliance with the organisation's information security requirements or non-compliance. Security practices may also come in the form of adherence to security standards or regulations, such as the 27002 standard.

Outcomes: represent the security-related effectiveness of information security management. This outcome (culture) serves as a desired output to protect the information properties of confidentiality, integrity, availability and accountability.

The theoretical rationale to support the influence of organisational culture, technological and national culture values is explained next.

3.4 The relevant values of the organisational culture

The relationship between information systems and organisational culture is the focus of many studies conducted in the information system domain. According to Schein's three level model of organisational culture, behaviours of members of an organisation could be driven by the employees relevant beliefs (Schein, 1985). Researchers have utilised Schein's three levels of organisational culture to relate elements of information security (Schlienger and Teufel, 2002, 2003; Zakaria and Gani, 2003; Vroom and von Solms, 2004; von Solms, 2005; Thomson et al., 2006). Findings from these studies indicate that organisational culture has a major impact on both information security management and organisational performance.

The management of information systems is considered a significant challenge. The two main aspects are at the governance level and the operational level. Information assurance governance gives organisational direction whereas operational management is concerned with ensuring the intent of the governance is achieved. Management issues include the formulation of direction policies, management rules, responsibility, awareness, commitment of senior management and existence of relevant policies. One can assume that managers in developing countries face many of the same problems that affect organisations in developed countries, but they also have other distinct challenges.

It is important to align the cultural values, beliefs and assumptions of users with the managerial practices (Hofstede, 1993). This research proposes that organisational cultural values, such as security-related management commitment, skills and training, awareness, information systems structure, information and knowledge sharing and change management, are reflective of managerial impact on information security. These values are chosen because information systems management standards (AS/NZS, 2006; NIST, 2006; OECD, 2002; ISO/IEC, 2005) as well as previous studies (Hackney et al, 2000; Moon, 2000; Norris and Moon, 2005; Siponen, 2000; von Solms 2000; 2006; Heeks, 1999) and reports such as the United Nations Information Economy Report 2005 (UN, 2005a), have found them to be important manifestations of information security management systems. Such values are expected to influence security-related behaviours/practices of an organisation's employees. Each of these values is briefly discussed and theoretical support is provided to justify the proposition linking managerial security values to information security culture.

Figure 3.2 shows the organisational culture values that influence security-related behaviours/practices of an organisation's employee. Table 3.1 summarises the organisational culture values and the related information security issues.

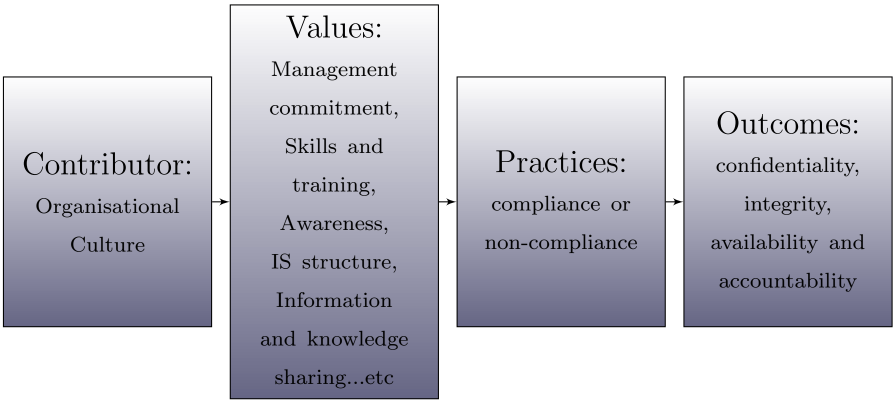

Contributor:
Organisational Culture
Values:
Management commitment, Skills and training, Awareness, IS structure, Information and knowledge sharing...etc
Practices:
compliance or non-compliance
Outcomes:
confidentiality, integrity, availability and accountability

Figure 3.2: Organisational cultural dimensions

3.4.1 Management commitment

Management commitment refers to the willingness of top management to provide the resources and support required for information systems success. The success of information security culture requires a strong and continuous management commitment (Knapp et al., 2006). Organisations can avoid losses related to computer breaches if more commitment and deterrence is given (Dhillon, 1999). The organisational commitment is affected by organisational culture, individual values, type of sector and managerial level as key determinants of organisational commitment (Moon, 2000). Key to the success of the commitment planning process is that commitments are defined and measured in objective terms (Singleton et al., 1988). Schein (2004) outlines that culture is the function of leadership at all levels

TABLE 3.1: Organisational cultural values

Organisational values	Description and potential effect	Study
Management commitment	Refers to the apparent top level support for the information security program. Organisations can avoid losses related to IT security if more commitment and deterrence is given.	(Cooper and Zmud 1990; Dhillon, 1999; Zakareya Ebrahim and Zahir Irani, 2005; Fulford and Doherty, 2003; Moon, 2000;Chia2002)
Skills and training	Refers to the development of relevant skills and knowledge in staff with information security responsibilities. Lack of IT staff skills, the high level turnover rates of IT staff and training can lead to failure of security program.	(Ho, 2002; Moon and Welch, 2004; Norris and Moon, 2005; Moon, 2002;Chia2002)
Awareness	This represents the availability of awareness programmers to ensure that personnel are aware of their security responsibilities and security issues. Lack of managers and users' awareness can leads to mismatch and produces misuse of information security systems program.	(Siponen, 2000a; Chia et al., 2002; Norris and Moon, 2005; Ebrahim and Irani, 2005)
IS structure	The extent to which information systems are structured or dispersed throughout an organisation has an impact on the effectiveness of information security management.	(Hussein et al.,2005; Currire, 1996; Heeks; 1999;Chia2002)
Information and knowledge sharing	There is a program for Information and knowledge sharing. Members of organisations are sharing security information and knowledge with each other.	Vroom and von Solms (2004)
Information security technology	Successful security program requires reliable and continued updating of the necessary information security technology. An example of the necessary security technology is Public-Key Infrastructure (PKI) and adequate encryption systems to prevent various attacks such as viruses, worms and spasms that aim to destroy or degrade the functionality of the network.	(UN, 2005a; Zakareya Ebrahim and Zahir Irani, 2005)
Change management	change management can be defined as managing change in organisations to produce an improvement in the information security management.	(Ostroff, 2006; Ward and Elvin, 1999; Ngo et al., 2005)

of the organisation to recognise and do something about an undesirable situation. It is in this sense that leadership and culture are conceptually intertwined.

3.4.2 Skills and training

Insufficient skills and training can lead to misuse of the electronic processes hindering the potential benefits that might be attained by an information system. Skilled staff and adequate continuous training programs have been recognised as an important value for the success of information security programs (Ho, 2002; Norris and Moon, 2005). Hinnant and Welch (2003) argue that increasing the level of computer self-efficacy through training or ICT specific education may serve to influence managerial perceptions of broader ICT initiatives within public organisations.

3.4.3 Awareness

Security awareness programs provide managers and users adequate knowledge to evaluate adverse consequences of security problems and take the appropriate actions to prevent and correct security breaches. Manager and user awareness are focal components to information security management effectiveness. In order to minimize end-user errors, Siponen (2000a) introduced a conceptual foundation for organisational information security awareness programs. Siponen concluded that in order to achieve an effective awareness program, such a program should satisfy the behavioural theory requirements and explain to the end-user why they should follow security guidelines. User awareness is always viewed as a focal component and challenge in any ICT system but in the context of developing countries this is a significant issue.

Another focal point is that senior managers and users may not be aware of the security challenges. Each one of them holds certain assumptions, attitudes and values towards the information system implementation and use processes. This can lead to a mismatch of priorities between the organisation and its staff as end users. As a consequence, the lack of senior managers' awareness might hinder their willingness to commit sufficient resources. On the other hand, there are the users who might misuse the system due to the absence of a proper awareness program.

3.4.4 Information systems structure

The information systems structure has an impact on the success of information security management. According to Heeks (1999)) there are three possible approaches to information systems responsibilities: Centralised decisions are taken at the most senior or central level; Decentralised decisions are taken at some level lower than the most senior, typically by individual work units within the organisation or even by individual staff; and core-periphery decisions are taken at both senior and lower levels, either separately or in an integrated manner. Heeks suggests that core-periphery is most effective for ICT usage and information systems development (Heeks, 1999).

A flat, decentralised, flexible structure is generally considered to be supportive of creative action and innovation (Hedberg, 1981; Meyer, 1982; Nonaka, 1994). Within a decentralised structure, information flows more freely in all directions, and interfaces with other functions are more easily worked as points of cooperation rather than divisive barriers to be overcome. This, in turn, facilitates cross-functional teamwork and dissemination of ideas (Garvin, 1993). A flat structure facilitates decision making both by granting more autonomy to all members of the organisation and by making access to superiors easier (Martins and Terblanche, 2003). Structural flexibility in terms of employee influence on work organisation, task prioritisation and procedures creates opportunities for individuals to take initiative and innovate (Hill, 1996).

3.4.5 Information and knowledge sharing

Integration is the extent to which there are coordination and control procedures across different functions of the organisation and other organisations (Scholl, 2003; Currie, 1996; Lam, 2005; Ebrahim and Irani, 2005). Bouthillier and Shearer (2002) stated that knowledge sharing ”involves the transfer of knowledge from one (or more) person to another one (or more)”. This suggests that information system processes for information and knowledge need to be effectively managed and consequently secured.

Issues such as different security models, data ownership and information security policy evolution have a negative impact on information security culture development and deployment. New processes of IT technology, at different levels within the organisation, demand full coordination between stakeholders. Procedures standardisation is required in order to integrate different internal processes, which demand very clear prior definition of leadership and respective function. Hence, the success of the use of a new process depends on the development of relationships and trust between stakeholders within the organisations involved.

3.4.6 Information security technology

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. Other properties such as authenticity, accountability, non-repudiation and reliability are also involved [ISO/IEC 27002:2005]. Security mechanisms are the technologies that provide the security services; for example digital signatures and firewalls. Technical infrastructure that is capable of handling the required volume and type of transactions in a secure manner is a necessity in achieving the information assurance objectives.

3.4.7 Change management

The primary purpose of change management is to assure smooth operational continuity and orderly evolution of the information system. Effective change management is necessary to ensure that all information system requirements are performed in a structured and controlled manner and provide management with a chronological history of all needed modifications.

By implication, change management in the information system management is also topical as systems go through development phases (Ostroff, 2006; Ward and Elvin, 1999). Grover et al. (1995) identified the key elements of change management as breaking the organisational status quo and introducing new practices, new values and new structures.

In this study's context, change management can be defined as managing change in organisations to produce an improvement in the information security management. However, organisations often face acute internal resistance when implementing new information and communications technology systems as employees may view this as a threat to their jobs. Initiating the need for change through a change management process will facilitate the achievement of information security culture. Organisations should plan their own information security plan and allow for its evolution through continuous changes in management programs.

In relation to the information security culture, very few approaches investigate the dynamic aspect of information security culture: i.e., how information security culture is generated and evolved and how change management can guide the organisation to produce an improvement in the information security management. Accordingly, the beliefs, norms and behaviour of organisations' members need to be engineered so that they are in line with specified security requirements. To this end, this research puts forward change management as a key component of the development of information security culture.

3.5 The relevant values of the national culture

To understand how national culture is related to information security behaviour, the current study defines four national cultural values in the conceptual framework. These could influence and shape information security oriented behaviours. The four national cultural values are: Power distance, Uncertainty avoidance, Individualism vs. Collectivism (Hofstede, 2001) and Context (Hall, 1976). Each of the four cultural values represents a set of underlying values and beliefs and assumptions

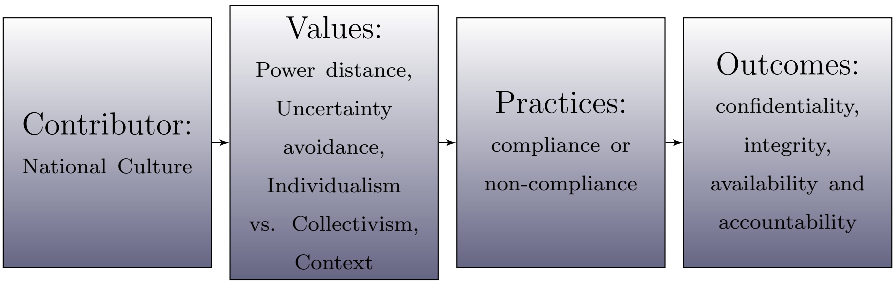


FIGURE 3.3: National cultural dimensions

which people may carry with them when they join an organisation. These values and beliefs of organisations members, in turn, influence the internal work culture facilitating certain security behaviours and inhibiting others. The current study has chosen to look at these four values in the context of Saudi Arabia, first, because of their perceived importance in the conduct of information security related practices and, second, because of the study's country-specific culture. Although the masculinity vs. femininity value (Hofstede, 2001) may influence information security behaviour, this value has not been considered in the current study. This is because the present study does not aim to validate Hofstede's cultural values, but rather explore the impact of social aspects on individuals' information security behaviour, which should be independent of sample size and gender. In addition, access to female employees in the Saudi Arabia context, at the time of this study, was expected to be very time intensive to process. This is in part due to distance and time constraints.

According to Hofstede (2001), industrialised countries are characterised by more individualism, a low power distance structure and a low uncertainty avoidance culture. By contrast, developing countries are characterised by more collectivism, a high power distance structure and a high uncertainty avoidance culture. The following discussion will examine how each value of the national cultural is likely to promote or hinder the security oriented behaviours with more focus on the characteristics of developing countries. Table 3.2 summarises the four national cultural values and the related information security issues and values. Figure 3.3 shows the national culture values that influence security-related behaviours of an organisation's employee.

Table 3.2: National culture values and relevant information security issues

Culture values	**Description of Value**	**Relevant information security issues**
National culture Hofstede (2001)		
Power distance	Power distance is the extent to which power is dispersed across the organisation.	Centralisation vs.decentralisation. organisation has a strong hierarchical structure. IT staff are authorised to make important decisions related to information security issues.
Uncertainty avoidance	Uncertainty avoidance is the extent to which the culture feels endangered by unfamiliar happenings.	Willing to take risk. Resistance to change.
Individualism vs Collectivism	Individualism refers to the degree of importance of an individual's requirements compared with the group's needs as a whole.	(+) impact on sharing security information and knowledge with others (-) impact on reporting information security incidents (eg. password sharing).
Context: Hall (1976)	High context cultures prefer a communication style in which individuals prefer to draw inferences from non-explicit or implicit information. Individuals in low context cultures prefer information to be stated directly and exhibit a preference for quantifiable detail.	Information security policy in place. It is documented in specific detail and communicated to all employees.

Power distance:

Power distance is the extent to which power is dispersed across the organisation. In high power distance cultures, employees expect more distant relationships with supervisors, and expect that supervisors will use a more directive leadership style compared to cultures with lower power distance (Hofstede, 2001). The relationships with and perceptions of supervisors are important in high power distance cultures. Individuals intend to follow the expectations of management and they are more likely to approve a system that they perceive to be supported by top management (Karahanna et al., 1999). Commitment of management should be more strongly related to overall organisation security culture in high power distance as compared to low power distance cultures. Thus, it is more likely that individuals accept the decisions and opinions of their supervisors due to their superior position (Clugston et al., 2000).

In relation to information security, this means that a low degree of tolerance may contribute positively to the information security culture. However, a low degree of tolerance has been associated with low employee involvement in decision-making processes. Lack of individual involvement has been linked to information system failure. One of the important values for effectively creating an information security culture is to involve employees in the setting of information security management goals (von Solms and von Solms, 2004a). A related issue of considerable importance concerns the impact of the power distance on the principle of accountability, and consequently this negatively influences the information security effectiveness of organisations. The impact of this value may lead to the fact that decisions of management go without questioning, for example, a top manager or IT staff member takes advantage of his position to compromise the rules (Dhillon and Backhouse, 2001).

Uncertainty avoidance:

Uncertainty avoidance is the extent to which the culture feels endangered by unfamiliar happenings. A high uncertainty avoidance ranking indicates that individuals have more concern about ambiguity and uncertainty and has less tolerance for a variety of opinions. This is reflected in a society that is more rule-oriented, less readily accepts change, and takes low risks (Hofstede, 2001).

This value reinforces the need to maintain the status quo and reject new ideas. Individuals from high uncertainty avoidance cultures are less willing to take risks and accept organisational change (Shane, 1995). For example, when faced with arguments of efficiency, management respond with claims of aspects of fear, uncertainty and doubt. Organisations take an incremental approach when they make a strategic choice of introducing new programs and innovations because incrementalism helps them minimise any potential risk. One would expect difficulty and resistance to change in implementing a new information security program or new policy.

Individuals in high uncertainty avoidance cultures appeared to have anxiety, to gravitate toward secure settings and to use experts (Hofstede, 2001). This suggests that outsourcing information systems would be a viable choice as people are willing to depend on IT experts rather than adopting an in-house strategy. This places a higher level of importance on issues that can be exploited in this fashion, such as implementing a disaster recovery/contingency plan for the information system. This trait may impact the principle of the availability if an organisation depends on contractors by outsourcing its entire information systems and is slowly coping with rapid technological changes and the associated threat.

Individualism vs. collectivism:

Individualism refers to the degree of importance of an individual's requirements compared with the group's needs as a whole. In individualistic cultures, employees act for their own interest rather than for the good of the group or organisation (Hofstede, 2001). In collectivistic cultures, employees would value the achievements of the organisation before the achievements of individuals. This cultural trait can affect the employees' reasoning for complying with organisational requirements (e.g. information security policy).

The notion of in-group attainments is more visible in a collectivist society, which may have practical implications in terms of the day-to-day individual's security practices. On the one hand, this would assist the information and knowledge-sharing culture within the organisation where individuals are willing to share security information and knowledge. Employees can exercise cooperative security practices by taking action about other acts that would jeopardise the information system by, for example, reporting unauthorized acts. On the other hand, it may lead to undesirable behaviour by compromising the principle of confidentiality in an information sharing environment (Chang and Lin, 2007), for instance, sharing passwords with others or not reporting a fellow staff member's unauthorised act. This suggests that the effectiveness of an information security system imposes paradoxical requirements in order to balance opposite cultural orientations. Implicit in this, is that people in a collective society may have the tendency to follow information security rules and procedures for the sake of protecting the interest of the group (organisation).

Context:

High context cultures prefer a communication style in which individuals prefer to draw inferences from non-explicit or implicit information. Individuals in low context cultures prefer information to be stated directly and exhibit a preference for quantifiable detail (Hall, 1976).

This can have practical implication in terms of the clarity of information security plans, policies and procedures. Users may mis interpret security policy if their roles and security requirements are not clearly specified. If security requirements are not clearly specified one would not expect them to be followed. This emphasises the importance of policy communication in high context cultures. A formal and well defined communication plan is required for information system success to prevent different interpretations of the information security policy. Effective information security policy has to be clearly documented and communicated to all employees (von Solms and von Solms, 2004b). Hone and Eloff (2002) stated that the effectiveness of the policy is dependent on the way the security contents are addressed in the policy document and how the content is communicated to all users .

3.6 Concluding remarks

In this chapter the conceptual framework describing the values influencing information security culture within organisations was developed. Based on the existing literature and past studies analysis, it is posited that information security culture is to a considerable extent a product of the interaction of all the internal and external aspects of the organisation. This is presented by encompassing the values of organisation and national culture, management activities, support mechanisms and individuals' behaviour.

The conceptual framework proposed introduces two new issues which have not received much attention in the information security literature. First, in this framework, national and organisational cultures are included as separate constructs to enable the examination of their values that may influence security related behaviours. This is incorporated by highlighting the possibilities of the influence of security-related values and beliefs of national and organisational culture on the belief systems of the organisation's members. Second, it has been argued that security culture in organisations is not a static process and needs to be managed through an ongoing base within the organisation. This is incorporated by proposing change management as a key component of the security culture development.

Clearly, the proposed framework requires further testing for thorough empirical validation. It is the intention that a case study approach will be carried out to capture the richness of the development processes of information security culture in selected Saudi Arabia organisations. Such a model substantially enhances our understanding of information security culture. By identifying the relevant values and their interrelationships, such a model may also better serve and guide practitioners, managers and those entities in direct contact with the organisational information security management within government and private organisations in successfully and effectively initiating and implementing information security culture.

3.7 Summary

This chapter builds on the existing evidence in the literature and the research questions for this study that arise from gaps in exiting work, as reviewed in Chapter 2 of this thesis. This chapter addressed the following issues. First, the theoretical foundation underlying the conceptual framework was highlighted. Second, the premises underlying the framework are elaborated and the key terms used in the framework were explained. Third, the framework was developed and the theoretical and/or empirical underpinnings of each relationship were discussed. Finally, concluding remarks on the proposed framework were presented.

Insights from the discussion in Chapter 1 and this chapter led to the development of the research methodology by adopting a case study method, which will be discussed in detail in the next chapter.

Chapter 4

RESEARCH METHODOLOGY

In this chapter, details of the research methodology used in the study are discussed. The chapter begins with a theoretical perspective of the research methodology. The background for the selection of this methodology is discussed. Then the case study protocol, including data collection procedures, is outlined. Lastly, data analysis strategy and process are discussed followed by a discussion of the validity and reliability issues.

4.1 Theoretical Perspective

"The research shall move from objectives and questions, to assumptions and design choices, to specific data uncovered, and finally, to results and conclusions" (Klein and Myers, 1999). The aim of this study is to provide a useful, integrated, practice-oriented and theoretically sound framework that will assist developers to succeed in the challenging task of developing and deploying an organisation's information security culture within the Saudi context. In particular, the research intention is to find and understand relationships between behaviours, attitudes towards specific factors and issues related to information security, knowledge sharing and change management to assess the overall state of information security culture.

The epistemological assumptions are concerned with the nature of knowledge and how it can be obtained. Crotty (1998) distinguishes between three epistemological positions: objectivism, constructivism and subjectivism. In objectivism, knowledge exists whether we are conscious of it or not. Researchers with this position look for causes and effects and explanations. They rely upon experimental, quasi-experimental and survey methods. The constructivist position on the other hand, assumes that knowledge of reality is gained through social constructions such as language, consciousness, shared meanings, documents, tools, and other artifacts (Klein and Myers, 1999). Findings are usually presented in terms of the criteria of grounded theory or pattern theories (Denzin and Lincoln, 2003). A researcher with a subjectivism position argues that understanding human behaviour can be achieved through reconstructing the self-understandings of those performing them. The concepts or practices in a particular context may seem obvious and natural but are actually artifacts of that context (Crotty, 1998).

The epistemological position for this research is constructivism. The proposed research approach is primarily explorative and interpretive in nature. The lack of systematic research of the information security culture phenomenon in the Saudi Arabia context justifies the exploratory nature of this study. Consequently this study has used an interpretive approach to research. The aim of interpretive research is to "understand a phenomenon from the point of view of the participants and its particular social and institutional context" (Kaplan and Maxwell, 1994). In an interpretive research method the context is considered as a main element as it aims at "producing an understanding of the context of the information system, and the process whereby the information system influences and is influenced by the context" (Walsham, 1993). Dhillon and Backhouse (2001) assert that an interpretive understanding of concerns about information systems security offers "advantages, furnishing a holistic view of the problem domain".

The underlying ontology of the approach used here lies in the interpretive paradigm. The ontology of this research with regard to information security management is that information security issues should be treated from a social-technical perspective. The social-technical approach is argued to be an important strategy for addressing organisational and social issues (Lyytinen, 1987; Iivari and Hirschheim, 1996). This current study contends that the information security culture factors and issues in an organisation should be examined against the frame of reference of the individuals associated with these factors and issues, and against the overall social context within which they occur. Hence, a qualitative research approach having philosophical foundations mainly in interpretivism is deemed appropriate for this study. Figure 4.1 illustrates the research's underlying philosophies, epistemology, ontology and method.

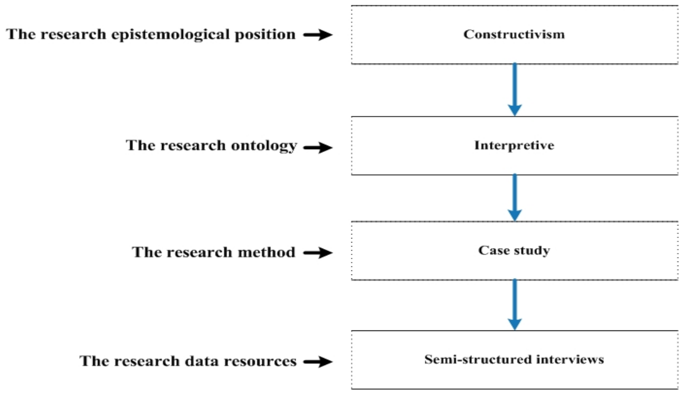

The research epistemological position
Constructivism
The research ontology
Interpretive
The research method
Case study
The research data resources
Semi-structured interviews

FIGURE 4.1: Research underlying philosophies

4.2 The case study method

As a research method, the case study originates in the social sciences, particularly in the fieldwork of anthropology and sociology (Walsham and Waema, 1994; Benbasat et al., 1987; Yin, 2003). Case studies in general "examine a phenomenon in its natural setting, employing multiple methods of data collection to gather information from one or a few entities" (Benbasat et al., 1987; Yin, 2003). The use of the case study as a type of qualitative method is well presented by much of the existing literature as an appropriate research method for answering 'how' or 'why' questions (Yin, 2003). Case studies are conducted from the positivist, post-positivist and interpretive stance (Walsham and Waema, 1994; Orlikowski and Baroudi, 1991). In the positivist stance, researchers contend that there is an objective reality that can be studied, analysed, quantitatively depicted, and thus understood. The post-positivists argue that there is no single objective reality, and that reality can never be completely understood. From the interpretive stance, used meanings are constructed by humans as they engage with the world they are interpreting and they make sense of the world based on their historical and social perspective. Researchers seek to understand the context and then make an interpretation of what they find, which is shaped by their own experiences and backgrounds.

Case studies generate knowledge of a particular set of results to a broader theory using analytic generalisation compared to statistical generalisation in non interpretive methods (Yin, 2003; Stake, 1995). Analytic generalisation, refers to the study of a phenomenon in its real context to support, contest, refine, or elaborate a theory, model, or concept (Schwandt, 1997). A number of interpretive case studies has been published in the information system literature, for exploring and hypothesising about information system aspects and issues (Walsham and Waema, 1994; Orlikowski and Baroudi, 1991). The scope of the case study ranges from individuals, to organisational groups, to national policies or events. Cases are compared and their characteristics are studied and behaviour patterns noted (Stake, 1995).

It has been proposed (Yin, 2003; Benbasat et al., 1987) that the case study:

1. investigates a contemporary phenomenon within its real-life context,
2. is suitable for answering the ‘how’ and ‘why’ questions and
3. uses interviews and documentary materials without using participant observation.

Stake (1995) identifies three types of studies using the case study method. In the first type, he identifies intrinsic case studies in which the researcher seeks a better understanding of the particular case. The second type involves using the instrumental case study to examine a particular instance to provide insight into an issue or refinement of theory. In the third type a number of researchers may jointly study a number of case studies in order to inquire into the phenomenon, population, or general condition.

The intention of this research is to find and understand relationships between behaviours and attitudes towards factors and issues of information security management, knowledge sharing and change management to assess the overall state of information security management. Hence, this research fits into the second category of Stake's (1995) classification. The instrumental case study method is adopted in this research as a strategy for three primary reasons.

First, the selection of the research method has been guided by the nature of our research objectives and by the type of research questions that have triggered this research, an approach that is widely suggested in the literature (Benbasat et al., 1987; Eisenhardt, 1989; Yin, 2003). It is the advantage offered by a case study in investigating a phenomenon within its real life context that makes this method the most appropriate (Yin, 2003; Stake, 1995). This research investigates in depth information security management culture elements and issues within their organisational context in the Saudi Arabia environment.

Second, a major application for the case study is to explore those situations in which the intervention being evaluated has no clear set of outcomes (Yin, 2003). Benbasat et al. (1987) point out that case study researchers generally have less a priori knowledge of what the variables of interest will be and how they will be measured and that the lack of a priori knowledge is sometimes a matter of degree. Hence, the lack of systematic research of the information security culture phenomenon in the Saudi Arabia context justifies the use of the case study method in this research.

Third, the data generated by case studies would often resonate experientially with a broad cross section of readers, thereby facilitating a greater understanding of the phenomenon (Stake, 1995). The case study method seemed particularly useful here given the complexity and multi-disciplinary relationships between cultural dimensions and information security management practices (Yin, 2003). Hence, the use of the case study method would allow the inclusion and investigation of these key organisational and cultural elements.

It is recommended that a case study protocol should be used as a guide in conducting case research (Eisenhardt, 1989; Yin, 2003). According to Miles and Huberman (1994) such a protocol should outline the procedures and rules that govern the conduct of the researcher and the research project. Hilangwa and Pervan (2005) have noted that there are very few established case study protocols published in the literature. They proposed a structure and content of the case study protocol. The case study protocol throughout this research follows the Hilangwa and Pervan (2005) structure and content with some modifications to suit the objectives and development of this study.

4.3 The case study protocol

4.3.1 General

The goal of this research is to provide a useful, integrated, practice-oriented and theoretically sound framework that will assist developers to succeed in the challenging task of developing and deploying an organisation's information security culture within the Saudi context. More specifically, the research focuses on the relationships between cultural and management factors(RQ1), issues and practices (RQ2), and recommendations for the improvement of information security management (RQ3) in organisations in Saudi Arabia. Yin (2003) proposed five components of case studies:

1. A study's questions,
2. Its propositions, if any,
3. Its unit(s) of analysis,
4. The logic linking the data to the propositions, and

5. The criteria for interpreting the findings (Yin, 2003).

The research questions framed as "what", "how", and "why" determine the relevant strategy to be used. In this study, the nature of the questions leads to an exploratory-explanatory case study. As suggested by Yin (2003), case studies may argue for the theoretical propositions or for developing a descriptive framework to organise the case data (Yin, 2003). This study being exploratory will rely on the research conceptual framework to investigate the information security issues and practices in three organisation in the Saudi Arabia context. The unit of analysis in a case study could be an individual, a community, an organisation, a nation-state or a phenomenon (Yin, 2003; Stake, 1995). This study uses the case study information security culture values and practices as the unit of analysis. The linking of the data to the conceptual framework and the criteria for interpretation of the findings will be presented in the data analysis and report. These five components will be further discussed in the remainder of this chapter.

The data will be collected through two methods. Interviews with participants from three Saudi organisations will be conducted and analysed and interpreted within the research analysis framework. Published documentation will be gathered and analysed. This will help to develop a model for public and private organisations to use as a recommended assessment tool in order to develop and deploy an organisation's information security culture within the Saudi Arabia context. This model will be designed to serve the needs of a variety of different audiences. Included among these audiences will be government agency managers, IT officers and researchers. The researcher acknowledges the importance of keeping a chain of evidence, a mechanism that is recommended by (Yin, 2003). Throughout this research, evidence from different resources will be collected and stored in the study data base for each case.

4.3.2 Procedures

In any empirical investigation, uniformity of method in data collection contributes greatly to rigor of method and validity of results (Miles and Huberman, 1994). In this research three in-depth case studies will be conducted to identify potential organisational elements needed to be addressed or managed to ensure effective information security management in organisations in Saudi Arabia. The literature review provides the initial conceptual framework. This is elaborated upon by the detailed documentation analyses of the three case studies. The interviews complete the exploratory investigation providing the necessary detail for the final conceptual framework. The initial conceptual framework incorporates the identified cultural dimensions of Chia et al. (2002) and Hofstede (2001). The intention is to relate a range of cultural values and their potential effects on effective information security management culture in the Saudi context. In this research the cases studied are in three Saudi Arabia organisations and the phenomenon of interest, unit of analysis, is information security management practices.

4.3.2.1 Establishing initial contacts

Given the nature of the phenomena under study, the physical distance between the researcher and the environment under study, and the absence of a previous systematic approach, some prior preparation was needed. In an attempt to establish initial contact with potential participants, a number of institutions were contacted about their interest in participating in this research by sending them a letter of interest (see Appendix B) or by visiting them personally. Those were organisations in a position to provide views on information security management issues and they usually have good records of advanced technology adoption. Organisations' environments should also have an e-government initiative in place or be planning to establish one. These are available on a limited scale, which makes the process pretty much straightforward. The three selected did have some kind of e-government initiative under these conditions. Those organisations invited to participate in the research ranged from government agencies to private and non-profit firms. In general, the results were positive. However, it appeared that private and non-profit firms were more interested and willing to help than public ones. The contact details for all contacted participants are stored on the research database.

4.3.2.2 Selection of cases

Yin (2003) points out that case selection should be guided by replication logic rather than statistical logic. It is expected that the selected sites should produce similar results (literal replication) or, on the contrary, completely opposite results (theoretical replication) (Yin, 2003). In light of this argument and the result of the initial contact process, three organisations were selected, to gather data related to the current state of information security management. These selected organisations have good historical records of advanced technology adoption. They are in a position to provide relevant views on information security management issues which are suited to the investigation of these research questions.

Semi-structured interviews with members of the selected organisations were carried out. The selection of the organisation's participants was in light of their qualifications and involvement in the information security management process in their organisations. A brief profile about each case follows:

1. Case A is a public-private company which has seven business units. Organisation A is among the world's market leaders in the production of different petrochemical products.

2. Case B comprised sixteen IT managers and staff from three public organisations in Saudi Arabia, where their organisations provide services for citizen and other organisations in Saudi Arabia. They represent public organisations that have successful e-government initiatives in Saudi Arabia.

3. Case C is a non-profit organisation that provides support services for private organisations in Saudi Arabia. Case C's main role is to represent the interests of its members and represent them among the concerned authorities.

Site visits	Interview duration and time	**Description**
1	One hour to one hour and a half. Between 9:00 am to 11:00 am	The purpose of this first visit is to conduct interview with the organisation CIOs and schedule the remaining interviews.
2	One hour to one hour and a half. Between 9:00 am to 3:00 pm	Conduct three interviews with three participants.
3	One hour to one hour and a half. Between 9:00 am to 3:00 pm.	Conduct three interviews with three participants.
4	Between 9:00 am to 3:00 pm. One hour to one hour and a half	Conduct three interviews with three participants.
5	Open	To follow up

Table 4.1: Initial Time Table

The research questions will be answered by analysing the responses from the organisation's participants. Although the selected cases operate in different contexts, the present study does not aim to present a representative picture of organisational information security measures, but rather explore relations between implementation, effectiveness of measures and impact of social aspects, which should be independent of sample size.

4.3.2.3 Scheduling of field visits

A major difference to other research methods in case study research is that the investigator does not control the data collection environment (Yin, 2003). The subject's schedule dictates the activity (Stake, 1995). Hence, this particular data collection process was used. It was anticipated that initially five visits to each site would be made and a total of thirty eight interviews with participants from the three cases would be conducted. Each interview would last between one hour to one hour and a half. Each of the three cases would be provided with a suggested flexible schedule so that individual organisation could make any necessary modifications to suit their participants' availability. Table 4.1 presents the initial time table for each site.

4.3.2.4 Research instrument

Research instruments have been selected in keeping with the view that social explanations and arguments can be constructed by laying emphasis on depth and complexity in data. Surveys and questionnaires may provide a broad understanding of surface patterns (Mason, 2002). However, they fall short of providing an in-depth understanding of the information security culture and management issues that this research is seeking. Myers (1997) indicated that qualitative research emerged from the social environment as a means for researchers to effectively study social and cultural phenomena which might not be appropriately addressed by quantitative instruments. It was therefore considered that using interviews in this research would allow the researcher to develop a more detailed view of the factors and issues affecting information security management.

There are three major interview types: structured interviews, semi-structured interviews and unstructured interviews. Structured interviews employ a formally structured schedule of interview questions, with each of the respondents being offered the same set of stimulus (Berg, 1989). On the other hand, unstructured interviews do not employ a standard schedule of questions but instead develop questions based on interviewee responses as the interview progresses. Semi-structured interviews employ predetermined questions with questions being asked in a systematic and consistent order. The semi-structured interviews provide the researcher with the flexibility to ask unscheduled questions based on interviewee responses. Hence, qualitative semi-structured interviews have been selected as the primary data collection method.

To collect the qualitative data for this study, semi-structured interviews were conducted with participants from three cases in Saudi Arabia. Each interview is divided into three parts. The first part is concerned with demographics and general information about the interviewee. The purpose of these questions is to establish the roles of both the organisation and the interviewee within that organisation. The next part is made up of fairly specific questions to cover aspects about how security is managed at their organisation. These questions were adopted from the relevant literature (Chia et al., 2002; ISO/IEC, 2005; Knapp et al., 2006; Chang and Lin, 2007; Ramachandran et al., 2008). The final part comprises very general questions. The questions are intentionally broad to allow the interviewee to formulate their own interpretation of the questions and to cover aspects that are not addressed in the second section and could not be obtained from the available documentation to obtain a more thorough view of the security culture in the organisation. The development of this research instrument involves three phases, as defined in the following sections.

Phase One: Development of the interview guide The interpretive approach expresses social life based on social interactions and socially constructed meaning systems, which can help researchers to understand human thought and action in social and organisational contexts depending on the cultural meaning system (Neuman, 1997). Following this view, this research aims to explore people's individual and collective understandings, reasoning processes and other significant factors which may impact upon information security culture development and deployment. Specific data collection questions from each of these perspectives are set out in Part (1) and Part (2) of the interview guide (see Appendix A).As suggested by Yin (2003), these will form a guideline. This guideline will be used during each interview to maintain the sequence of questions and the level of consistency of each interview. Open-ended questions provided a frame of reference, and established depth without steering responses. Responses from interviewees are open-ended. This will allow respondents to provide details necessary to understand the richness of the phenomenon.

As Yin (2003) suggested, an interview guide has been developed and was used during each interview. An initial set of 20 questions was used as a guide in these interviews but the exact number and wording of the questions had the potential to be modified after the pilot phase. The questions were grouped in two sections (see Appendix A). Section One consists of five highly-structured questions to elicit specific information from the participants: their education, their job title/level, their department, the number of employees in their company and the organisation industry sector. Section Two consists of 10 flexible questions to elicit:

(1) information security related beliefs; (2) information security oriented behaviours; (3) beliefs about management's commitment to security; (4) perspectives about complying with hierarchy, rules and procedures, (5) beliefs about the importance of rewards and its influence on the security related beliefs, (6) beliefs about risk taking, (7) beliefs about management's commitment to data sharing; (8) perspectives about data sharing issues and security related issues in the organisation; and (9) attitude towards following managerial directives.

It has been designed in this manner to minimise potential bias through the application of common instruments, including the interview guide and supporting organisation documents. Miles and Huberman (1994) assert that comparable interviews can assist in building theory, improving explanations and contributing to recommendations and better practice.

To keep with the above view, and to acknowledge the need to retain fluidity of the interview process, the open-ended interview questions were chosen. Further, additional questions would be asked when appropriate based on the responses of the interviewees. This was to allow the participants to discuss pertinent themes in a suitable manner and to gain in-depth responses.

Table 4.2 presents the open-ended interview questions and their linkage to the research questions. Figure 4.2 illustrates the question tree and its interrelationships. Participants' answers to the interview questions (IQs) were designed to answer the research question (RQ) collectively. The answers to the RQs, taken collectively, should answer the research main objective ROBJ.

Phase Two: Pilot study (testing the interview protocol): As defined by Alreck and Settle (1995) a pretest is a preliminary trial of some or all aspects of the instrument to ensure that there are no unanticipated difficulties. Pilot studies may be done for one or more of the following reasons: to determine the appropriate

Table 4.2: The interview questions and their linkage to the research questions

Research Questions (RQ)	**(RQ1) What are the current management practices in relation to information security management and influencing cultural factors in Saudi Arabia?**	**(RQ2) To what extent do both dimensions of organisational and national culture have to be considered when dealing with information security management effectiveness in developing countries?**	**(RQ3) How can organisation achieve quality and successful development of information security culture that satisfy requirements in the Saudi context with respect to the proposed framework?**
Interview Questions (IQ)	Structured interviews instrument administrated to 38 participants from the three cases and case documentations and materials (see interview guide-Appendix A)	1. Do you think personal culture (i.e. values and beliefs) influences the security related behaviours? If YES, have these values and beliefs affected your staff's security-related behaviours? If so, in what aspects? Can you provide examples? If NO, can you expand? 2. Do you think information security related behaviours of members of the organization has been influenced by the managerial security initiatives like policies, guidelines, procedures, training programs? If YES, on what ways has it affected your staff's adherence to information security policy? If NO, what makes you think so? 3. What is your view on the quality of cooperation/communication your organization has with the: a) users and b) with the top management? 4. Do you believe that members of your organization share information and knowledge with IT staff and other colleges voluntarily? If YES, what are the factors that most influences this to happen in your department? If NO, what are the factors that most influences this not to happen in your department? 5. When it comes to making decision what level of guidance do IT staff need from upper management? Can you comment on the procedures of action when security issues arise? When the rules are not clear with respect to information security, or if there is no rule for a situation with respect to information security, how would that be handled by your department? Can you provide examples? 6. Do you believe the information management standards serve a useful purpose in managing your information security effectively? If YES, how? If NO, why? 7. What motivates the members of your organization to comply with information security policy? 8. How do tangible rewards (such as money, promotion) compare to intangible rewards (such as satisfaction and appreciation) 9. Can you comment on the procedures of action when resistance to security measures has come about? 10. What other specific information security related issues and factors do you see and encounter in terms of the effectiveness of the information system in your organization?	As RQ1 and RQ2 are answered and explored in the course of the research, it will become apparent how the objective of this question will be answered.

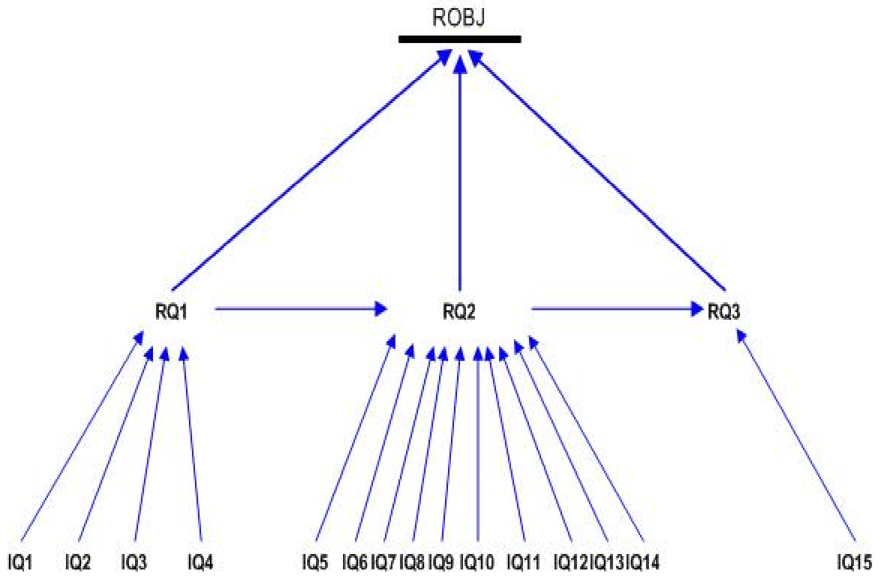


Figure 4.2: Questions Tree

unit of analysis, to refine the data collection instruments and / or get familiar with the research phenomenon (Yin, 2003).

In this research, the interview instrument was pretested, in Australia with six PhD students from Saudi Arabia who have a position in IT departments in different organisations in their country. The goal of this process was to see if the questions were tapping into the same overall phenomenon (content validity-section 4.3.4) and whether variations in the phrasing elicited similar responses (construct validity). Also this process ensured that the interview questions could be understood and measured validly. Based on the comments received from the pretest, modifications were made to the interview questions for improving their clarity before using it in the actual interview.

Analysis and results of the pilot study: The interview questions were pretested, with this group because they were believed to have a basic understanding about the Saudi Arabia context due to their close relationship with information security issues. The goal of this process was to see if the questions were tapping into the same overall phenomenon and to ensure that the interview questions could be understood and measured validly. This process also was executed in order to determine if what was intended to be captured is in fact what the data reflected.

This was important to ensure that the amount of data would not overwhelm the researcher, as well as to ensure that the researcher remained focused on the original purpose of the research. This pilot phase was undertaken in two rounds of interviews.

Round (1) involved open and broad questioning around each of the framework components, probing the participants' views on information security-related issues. These were guided by an interview protocol, which, in turn, will be informed from the data collection questions and comments raised by each participant. The data collected from *Round (1)* and the comments and suggestions were collected and analysed. In the course of conducting these interviews, gaps between the preliminary interview questions and the required data were identified. Two questions were dropped to eliminate a redundancy mentioned by more than one respondent. As a result, the interview guide was modified and divided into two sets of questions to incorporate the participants' comments and to overcome some of the shortcomings (see Appendix B). The two sets were designed to be complementary to each other and to provide a cross-check on the discoveries.

In the first set, a fixed set of questions was developed to capture the organisation's actual practices, in the form of a questionnaire (in Yes, Partially, No format). A 'Yes' answer indicates the practice is implemented. If the answer is 'No', it indicates the practice is not implemented at all. 'Partially' indicates that part of the practice is implemented. It was included (Partially answer) because some respondents may be unwilling to answer a "problem" question. Several participants raised this issue, for example one participant commented:

"it is hard to believe you would get an honest or accurate answer for this kind of question".

Hence, a choice of "Partially" was added to the first set questions to get more accurate answers. Grouping the closed (Yes, No) type of questions in one set aided in focusing more on the open ended questions to acquire an in-depth perspective about the issues. This process was also useful for easy reading and completion and to shorten the time needed for each interview.

The second set of questions was made of open-ended questions. Open-ended questions were designed to probe for an in-depth perspective about the issues. The set consists of two types of questions; the first type includes questions that evaluate and rate the relative importance of the various dimensions of the research framework and the second type assess qualitative indicators and elicits comment on some of the issues. Minor wording changes were implemented to improve the clarity of some questions. The end product included a small number of closed, demographic questions, three questions that evaluate and rate the relative importance of the information security issues and nine open-ended questions.

Round (2) In this round, the two sets of questions were used as a guide. Using a semi-structured interview, the participants completed the first set of the protocol questions concerning the organisation's actual practices, made up of nineteen questions in a closed configuration and twelve open ended questions. Each interview lasted over 40 minutes. Together, the qualitative and quantitative data obtained from the closed questions generated enough information to allow an in-depth analysis of the results.

The set of questions were revised for a final time to tighten it further by merging some questions which had similar themes and dropping some duplicate questions. The end product is attached as Appendix B.

Phase Three: Conducting the actual interviews: This final phase involved conducting and documenting the actual interview process with the three cases' participants. Actual interviews were based on the interview guide (see Appendix A). The interviews were mainly conducted face-to-face at the user's workplace in Saudi Arabia during the months of March 2009 and July 2009. The researcher conducted the interviews in English, though some Arabic terms were used where necessary. Prior to each interview, the study information background and the interview questionnaire sheets were provided to all participants. On the day of the interview and prior to initiating the actual interview phase, the rights of each participant were reviewed and the researcher assured them of the confidentiality of their responses. Each respondent was offered the opportunity to review the data recorded as well as the individual case study narrative within the research thesis. All comments, changes and modifications required by the participants were considered and reflected in the final case study report. In this research, all information of the participant's organisations will be anonymous. Thus, the case study will not contain specific information about the organisation and participants' names or references.

4.3.2.5 Published documentation

The use of more than one data source is a technique known as triangulation that is highly recommended by many researchers, such as Yin (2003), and Miles and Huberman (1994) as a mean for increasing both the reliability and validity of qualitative research. To help ensure reliability, secondary data sources were also used in this research, primarily consisting of associated organisation and public documentation. This includes formal documents such as policies, organisational charts, regulations and annual reports.

4.3.3 Analysis

Case studies generate a great amount of data that need to be analysed sufficiently and with appropriate techniques in order to be useful. In case studies, the collected data are analysed as they become available and the emerging results are used to shape the next set of observations. According to Yin (2003) analysing qualitative data is about examining, categorising, tabulating and recombining the empirical evidence to address the initial relationships as identified in the theoretical framework and to further identify new concepts and relationships. Miles and Huberman (1994) argued that by developing analysis strategies and techniques a priori, a researcher is forced to consider the data that would be collected and its relevance to the research. Yin (2003) suggested that a case study data analytical procedure consists of three steps:

- Step (1) choosing a general strategy to help in deciding what to analyze and why it should be analysed.
- Step (2) coding of the evidence.
- Step (3) using an analytic technique to develop or test the theories.

4.3.3.1 General analytic strategy

Analysing the content of interviews and observations is the process of identifying, coding, and categorising the primary patterns in the data (Patton, 1990). Yin (2003) describes two general analytic strategies for case study research. The first strategy relies on the theoretical propositions to organise the case study data; the second strategy argues for developing a descriptive framework to organise the case data (Yin, 2003). Following this suggestion, the second strategy of using a descriptive framework to organise the case study data has been adopted to serve as a guide to this research. In this study, the empirical material was analysed through categorising and identifying themes from the data. The categorisation of the data includes the interview transcripts, organisations' documents and published reports. At the first stage of categorising, the researcher relyed on categories derived from the conceptual framework. The conceptual framework components was used loosely. This allowed the researcher to be open in case the gathered data suggested other factors or issues. The data analysis process in this research is illustrated in Figure 4.3. This process involves five steps:

1. The first step began with the priori coding of themes and patterns based on the case research instrument(s) (Yin, 2003). The pretest of this research instrument outcome served as a priori coding of themes and patterns. These codes were later used in the analysis of individual transcripts.

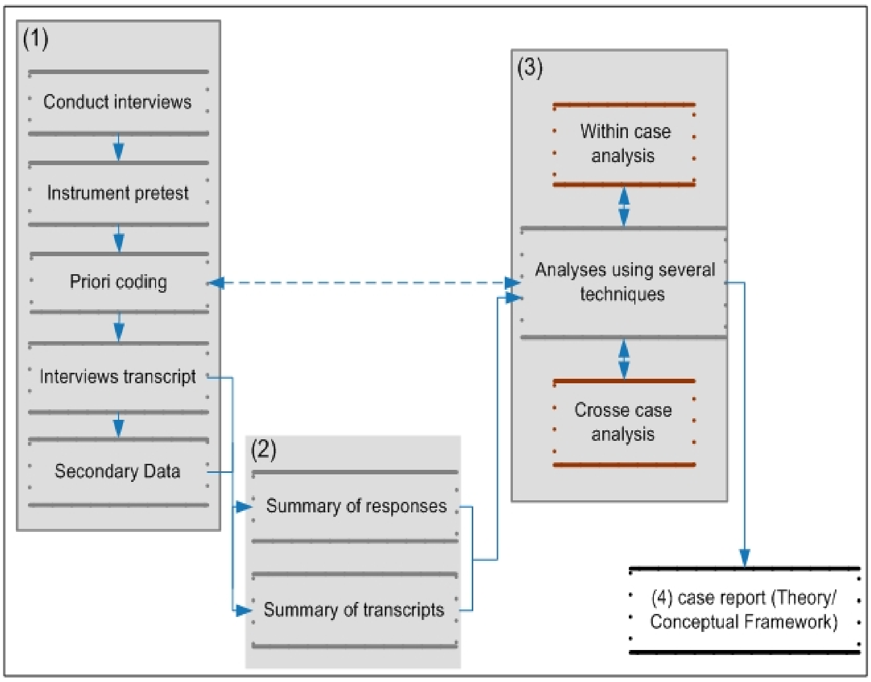


Figure 4.3: Data Analysis Process

2. Each individual transcript was summarised. These summaries were generated from each participant's interview transcript. There was also a summary for each case study. These summaries were created from each case response. This process was an analytic technique known as 'reduction'. This would help in developing a clear picture of participants' responses to interview questions (Miles and Huberman, 1994). Then all participants' individual responses to each question were combined in a single document. This process woul generate a case response summary that would help to make a comparative analysis of participant responses.

3. Transcript and response summaries were used for 'within-case' analyses and for 'cross-case' analyses respectively.

4. The final step involved drawing conclusions and writing the case study report.

5. In addition, an analysis of secondary data was conducted in parallel to the analysis of interview transcripts described above.

4.3.3.2 Analytic and coding techniques

There are two approaches used in qualitative research: inductive and deductive. Inductive studies usually begin with a loose research question rather than with a strict hypothesis. Data are then gathered and analysed through inductive rather than deductive principles. Quantitative research relies on the deductive method. The researcher collects data to test a predefined hypothesis. Deductive reasoning leads researchers to measure relative attainment of predetermined, clear and specific goals. Inductive reasoning leads researchers to focus more on program or product impacts and effects. Several researchers have followed a scheme in which deductive and inductive reasoning were combined. Hilangwa and Pervan (2005) suggested that data from multiple sources should be analysed using both techniques to achieve "a convergence on a given set of facts".

In this study the two techniques were applied. The deductive technique was applied when investigating the information security management factors and issues, moving from high-level to low-level factors and issues. The inductive technique was applied when using the organisations' issues to investigate and analyse the whole country's situation and draw recommendations.

Pattern codes represent the sets of emergent codes that the researcher develops during data analysis. They identify an emergent theme or pattern or explanation that the data from the site suggests to the researcher. Pattern coding serves two main purposes for case study research. First, it helps in reducing the large amounts of data into a small number of analytic units, and second, it acts as a tool for the researcher to develop a cognitive map of the events and processes happening in the site (Miles and Huberman, 1994).

Campbell (1975) points out that pattern-matching is a useful technique for linking data to the propositions. As recommended by Yin (2003) pattern matching was used to verify the concepts and relationships among concepts identified in the conceptual framework.

Also the captured data was analysed using suitable qualitative research software. The purpose of this was to reveal reveal patterns of events that were related to the factors and issues indicative of successful information security culture development and deployment.

4.3.4 Validity

The quality of case study research relies on the satisfaction of several criteria that have to be taken into account (Yin, 2003). These criteria are: construct validity, internal validity, external validity and reliability. Table 4.3, summarises the four criteria and presents the applied tactic in the current study.

4.3.4.1 Construct Validity

Construct validity is concerned with establishing appropriate operational measures for the constructs being studied. It has been suggested that three principles for data collection aimed at ensuring the construct validity of the study are adopting triangulation, developing a database of gathered data and maintaining a chain of evidence (Patton, 2002; Yin, 2003). These processes were adopted throughout the data collection and analysis phases as follows:

1. *Use of multiple sources of evidence:* case study research provides the researcher with the opportunity to employ multiple sources of evidence (Yin, 2003). The use of more than one data source is a technique known as triangulation, that is highly recommended by many researchers Miles and Huberman (1994) and Yin (2003) as a mean for increasing both the reliability and validity of qualitative research. In this study, the three case studies present multiple-sites that can provide such triangulation. In addition, the interviewing of multiple individuals in each organisation and information from documents and observations helped to triangulate further.

2. *Establish chain of evidence:* Yin (2003) argues that the chain of evidence of the case study allows the reader "to follow the derivation of any evidence from the initial research questions to ultimate case study conclusions". If the chain of evidence remains intact and functional, the case study will have addressed methodological problems of construct validity and reliability (Yin, 2003). In this study, establishing a chain of evidence was maintained through several ways. First, by creating a thorough case study database and by allowing the

Table 4.3: Criteria for evaluating the quality of case study research Based on Yin(2003), and the current study tactic

Criteria	**Technique**	**Phase of the research**	**The current study**
Construct validity	-Use of multiple source of evidence -Establish chain of evidence -Have key informants review draft case report	Data collection	-Three case studies present multiple-sites that can provide such triangulation. Further, the interviewing of multiple individuals in each organisation and information from documents and observations helped to triangulate. -First, by creating a thorough case study database and by allowing the research questions to constantly guide the data collection process. Second, a detailed narrative of the case study was created to provide the reader with a clear structure of the sequence of events. Third, care was taken to follow the procedures and guidelines set in the interview protocols.
Internal validity	-Do pattern matching -Do explanation building -Do time-series	Data analysis	-Pattern-matching was used. -A comparison between the cases was conducted and the emergent findings were linked to existing literature. -Factors affecting the phenomena were weighted.
External validity	-Use replication logic in multiple-case studies	Research design	-The same set of questions and process were applied to the three case studies. Also, a comparative process within each case study and between the three cases (cross analysis) was conducted to find any sort of recurring regularities.
Reliability	-Use case study protocol -Develop case study database	Data collection	-A case study protocol has been developed and employed. -Secondary data sources are also used in this research. -A case study database was developed using NVivo8.

research questions to constantly guide the data collection process. Second, a detailed narrative of the case study was created to provide the reader with a clear structure of the sequence of events. Third, care was taken to follow the procedures and guidelines set in the interview protocols.

3. *Validation of coding scheme:*

   A qualitative software was used to assist with effectively managing the data for intensive scrutiny and analysis. In this section, an overview of the tool's basic functionality and how it was utilised in this research is highlighted.

   The qualitative data software NVivo8 provides ways of helping the researcher develop and relate categories (the nodes) during the analyses process. NVivo also was helpful in storing ideas relevant to these categories, as well as modifying categories and their coding incrementally, as they emerged from the data. The coding and searching were the functions primarily used from the NVivo8 software during the analysis. Although the software was a useful tool, it could not code and organise the data without researcher input. Hence, an extensive effort from the researcher's side was necessary to link the data to the corresponding categories and themes.

   In this current study, coding was an iterative process that involved constantly revisiting the categories and linking data to the research framework categories. An advantage of this iterative process was that each participant and case record was reviewed many times as we moved between coded segments of text and the original records. The data from all three case studies was combined and coded into sixteen initial categories, corresponding to the research framework components. These first 16 categories were stored in NVivo8 as free nodes. The initial categories for coding the data were the twelve categories that were related to organisational culture values and four more categories that were related to national culture values. In this analysis stage, all of the data collected from interviews and documents was coded and put into one of these categories. The following two extracts were both coded into the category management commitment, which is part of the theme organisational culture values:

> *"We can't do what we did without their support, they value what we said and what we suggest.."*

> *"The top management already granted the authority to the IT staff to take a decision, of course within the organisational policy, rules, guidelines and procedures."*

Some data extracts were coded into more than one category simultaneously if there appeared to be multiple ideas within the text. For example, the following extract was both coded into the category of management commitment which is part of the theme of organisational culture values and into the category of power distance which belongs to the theme of national culture values:

> *" The top management already granted the authority to the IT staff to take a decision, of course within the organisational policy, rules, guidelines and procedures."*

The first part of the above quote indicates that top management provides support to IT staff in terms of decision-making. The second section of the quote indicates that while IT staff were authorised to take information security decisions it was constrained by the approval of upper management and by the organisation's rules and procedures.

An advantage of working within these early categories allowed us to observe potential linkages between the data, the sixteen categories and the six themes and any interrelationship between them. The themes form the basis of the results and discussion chapters. In the analysis stage, data from all of the resources were continuously re-examined and presented under these six themes:

(a) Influence of national culture values

(b) Influence of organisational values

(c) Influence of technology

(d) Practices

(e) Outcomes

(f) Change management

4.3.4.2 Internal validity

Internal validity is concerned with the degree of researcher inferences regarding cause-effect or causal relationships. Internal validity is a concern only in causal (explanatory) cases. This issue can be dealt with using pattern-matching, which has been described in a previous section (Section 4.3.3.2), as recommended by (Yin, 2003). Eisenhardt (1989) also suggested that linking the emergent theoretical propositions to existing literature enhances the internal validity of theory building from case study research, as applied in this study.

4.3.4.3 External validity

External validity is concerned with the generalisability of the findings of the case study (Yin, 2003). External validity deals with the investigated sample and whether the conclusions reached can be generalised beyond the sample (Boudreau et al., 2004). Yin (2003) suggests the use of replication logic to increase the external validity of findings in a multi-site case study. The replication process is an iterative process of pattern matching across subjects. The replication logic was achieved in this study, through conducting a comparative process within each case study and between the three cases (cross analysis) to find any sort of recurring regularities.

4.3.5 Reliability

The reliability of a study ensures that errors and biases in the study are minimised. Reliability requires that the process of research as applied in the study be consistent, allowing any later researcher to follow the exact same procedures and get the same findings (Yin, 2003). Yin (2003) suggests case study protocols and the development of a case study database to ensure reliability in case study research. To keep with this view, a case study protocol has been developed and employed.

The use of more than one data source is also highly recommended as a means for increasing qualitative research reliability (Miles and Huberman, 1994; Yin, 2003). Miles and Huberman (1994) stated that in order for the findings of the research not to be a result of "idiosyncrasies" of the research setting, multiple cases should be used. To help ensure reliability, secondary data sources are also used in this research, primarily consisting of associated organisation and public documentation. This includes formal documents such as policies, organisational charts, regulations and annual reports.

4.4 Summary of research methodology

The details of the research methodology and data collection methods are presented in this chapter. This chapter justified the choice of the case study method in that it is particularly useful for the current study given the complexity and multi-disciplinary relationships between cultural dimensions and information security management practices. Hence, the use of the case study method would allow the inclusion and investigation of these key organisational and cultural elements in an unexplored context. The data collection procedures, and a discussion of the data analysis procedures and strategy was outlined and justified. The chapter concluded with the methods to ensure reliability and validity aspects of the study.

The next chapter presents the findings of the study aimed at eliciting and synthesising current information security culture values and practices from the three case studies.

Chapter 5

ANALYSIS and RESULTS

This chapter presents an analysis of the qualitative data collected for this study. The chapter is divided in two sections. The first section gives a detailed description of each case sites and an analysis of the data collected in order to form a view of the information security culture of each organisation and the values influencing its security culture. The second section presents a cross case analysis of information security values and issues identified in the three cases.

The findings presented in this chapter are derived from interviews with case participants and an analysis of secondary information about each case's organisation. The secondary information includes annual reports, policy documents, organisational structures and press releases.

Each case issue is presented with a quote from the participant, which reflects the respondent's view of the issues. The values and issues are organised into the major categories corresponding to components of the research's conceptual framework on the information security culture development (refer to Figure 5.1).

The research question aims to identify the organisational and national cultural values and factors that have influenced the implementation and impact of information security management. The research conceptual model (from Chapter 3) is represented here to provide a focus for the case practices and issues.

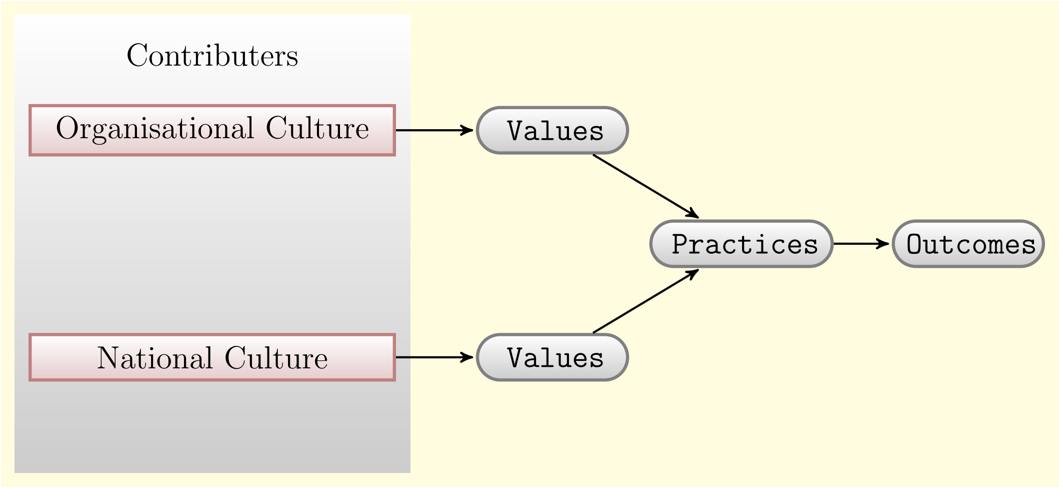


Figure 5.1: Research Conceptual Framework

5.1 Overview and analysis of the cases

In this study, efforts were made to select for case studies, organisations that allowed for data to be collected about a range of businesses, sizes and approaches to information systems security management. The three cases for the study were selected to represent private, public and non-profit sectors. They will be referred to as Case A, Case B and Case C, respectively. In this research, all information that may identify the participants or their organisations will be anonymous. Thus, the case study will not contain specific information about the organisation and participants' names or references. Instead, each participant's response will be assigned a sequential number, for example, [P5-A] (where P5 = Participant number five and'A' refers to participant's organisation, in this example, participant five belongs to Case A).

To understand the information security culture in an organisation, it is important to understand first its information security environment, practices and issues. Using a semi-structured interview, the participants responded to the first set of the protocol questions concerning their organisation's actual practices. There were fifteen questions in a structured questions and ten open ended questions and responses were recorded. Each interview lasted at least 40 minutes. Specific details of the interview data collection method and process have been presented in Chapter 4, Section 4.3.

The following subsection is structured as follows:

Firstly, general information about each case and the organisational structure of each case organisation is presented. It should be noted that the case description presented in this study relied on the organisation's documents (e.g. organisational charts, policies, annual reports), whereas the information security practices emerge from coding the interviewees' responses and from the quantitative data obtained from the closed questions.

Secondly, there is a discussion of the organisations' cultural values influencing the organisation members' beliefs and practices related to information security behaviour (see Figure 5.2).

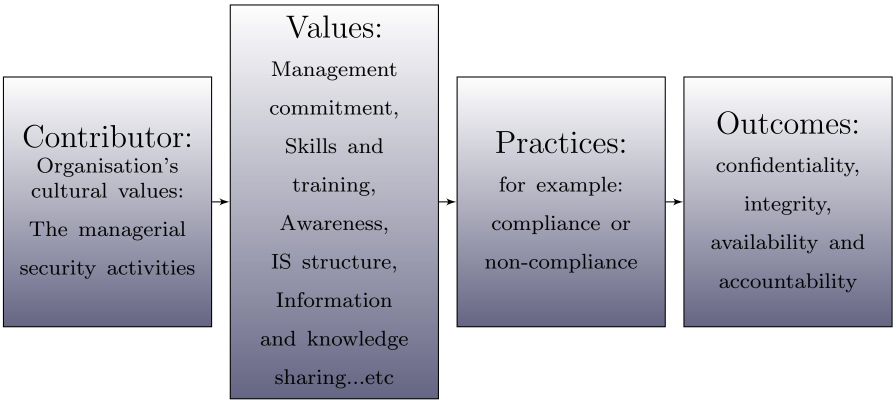

Contributor:
Organisation's cultural values:
The managerial security activities
Values:
Management commitment,
Skills and training,
Awareness,
IS structure,
Information and knowledge sharing...etc
Practices:
for example:
compliance or non-compliance
Outcomes:
confidentiality,
integrity,
availability and accountability

FIGURE 5.2: Organisational Cultural Dimensions

As discussed in Chapter 3, organisational culture is conceptualised to represent activities and factors related to the effectiveness of information security management. Information security management activities are those that managers practise or believe that they and their organisation should be practising to protect its information assets. They collectively describe the operational activities performed by the organisation and its members that support the existence and/or attainment of the information security culture. Specific details of the interview data coding process have been presented in Chapter 4, Section 4.3 and Appendix C.

Thirdly, national cultural values influencing the organisation members' beliefs about information security are discussed. This is conceptualized by the four national cultural values of (Power distance, Uncertainty avoidance, Individualism vs. Collectivism) (Hofstede, 2001) and Context (Hall, 1976), which are believed to have influence on the security-related behaviors of an organisation's employees.

5.2 Case(A)

According to Case A's annual report available in 2006, Case A is a public-private company with over 5000 employees. Case A is among the world's market leaders in the production of petrochemical products. Much of the success of Case A's industrial projects is associated with its policy of acquiring technology through joint ventures. The need to train its employees to operate the plants and make top quality petrochemical products, is one of its key challenges. To realise this goal, employees are sent abroad, mainly to the US, to undergo training in a wide range of specialties including IT and technical training. Today, nearly 80% of Case A's staff are highly qualified and well trained Saudi citizens. Almost all the top management of Case A are tertiary educated and hold a higher degree relevant to their position.

TABLE 5.1: Position and number of interviewees interviewed in Case A

Job position	Number of interviewees	Responsibilities of interviewees
IT department managers	3	Strategic policymaking in organisation, selecting information systems.
Information security officer	1	Strategic policymaking in organisation, selecting information security systems.
IT staff	6	Steering the IT implementation, providing support for end users, performing help-desk duties, maintaining functional and technical administration of the system and analysing ongoing use of the system.
Department managers	3	Working with the information system on a daily basis.
Total	13	

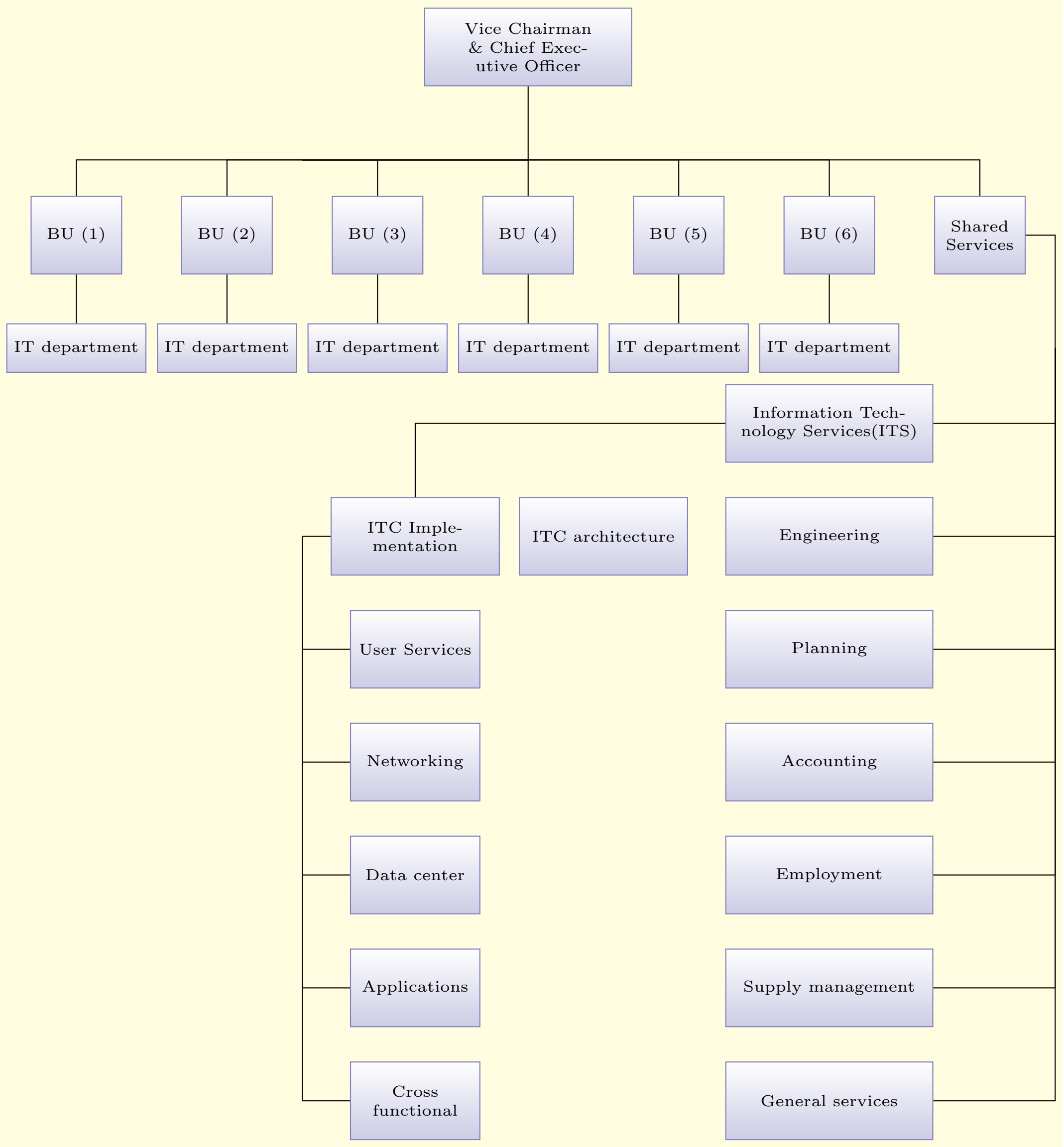


FIGURE 5.3: The organisational structure of Case A and details of its functions

Information technology services are provided through the Information Technology Services (ITS) group, which resides under the Shared Services unit. The ITS group comprises two departments: ITC architecture and ITC implementation. The organisational chart shows that each business unit has its own IT department[1]. The IT department managers of each unit report security related issues to their counterparts managers in the ITS group. Two of the IT managers in those business units were interviewed for this study. Table 5.1 overviews the number of interviews conducted during this case study.

[1] The organisational chart shows only the IT department of each business unit. It should be noted that there are other functional departments (e.g. Planning, Finance, HR etc.)

Table 5.2: Organisational values influencing the development of information security culture in Case A

Values	**Practices**	**Outcome**
Management commitment	Top management considers information security an important organisational priority. There was an allocation of resources to support its information security management. IT's decisions are approved and there is allocation of necessary resources. Information security aligned to organisation's overall strategies.	Consistent enforcement of information security rules appears to be achieved. Department's managers are committed to information security issues. High level of co-ordination among departments is evident.
Information Systems structure	Well-structured IT department. Information security responsibility lies with one department. Officer of Information Security has been assigned. Standardisation of information security approach, process and IT technology	One individual department can be held accountable for the information security incidents that might occur within the organisation. A quick response to IT department's requests and information security issues is likely to be achieved. Reduction of direct costs associated with IT, as in buying goods and services, or indirectly through developing and maintaining focused and uniform expertise. Facilitate the role of immediate managers and enhance the level of cooperation
Skills and training	There is a specific budget allocated for information security training programs. Training programs were limited to key managers and staff of the IT department. Inadequacy of in-house expertise.	Low level of information security culture among people at the lower level. Reliance on a third party. A portion of information security is controlled by a third party. Confidentiality and availability might be compromised.
Awareness	There is a formal awareness program (e.g. hotline, email notices, and the monthly Company General Committees meetings). Direct involvement from the finance and human resource departments. There is a specific budget allocated for information security awareness and training pro- grams. Awareness activities take a proactive perspective.	There was a clear understanding of the importance of information security and potential consequences of most individuals' security related actions. Information security messages are well communicated to prevent deniability. At the low level, more awareness programs are needed.
Motivations	Adoption of KPI's approach as a motivation mechanism, along with technical countermeasures.	Individual's loyalty is increased. Motivated individuals likely to comply with information security procedures and rules.
ISM policies and standards	International Information Security Management Standard ISO 27002 and has certified against it.Two forms of auditing: internal and third party auditors to conduct security-specific audits.	ISM standard was seen to help in technology selection and security provisioning. Ensure that their information security program standards are being applied and followed. Keep employees aware of information security responsibilities.

5.2.1 The influence of organisational culture values in Case A

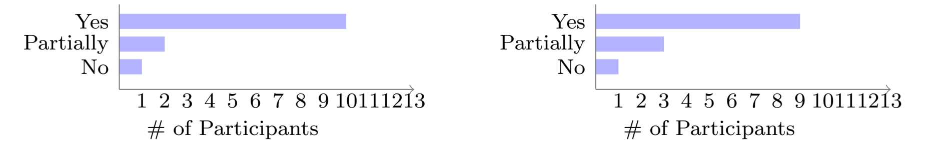
In this section the organisational culture values influencing the organisation members' beliefs and practices related to information security behaviour are presented. As discussed in Chapter 3, organisational culture values, that were generated from the related literature, were conceptualised in the research model to represent activities and factors related to information security culture deployment and development. On the other hand, the practices and possible outcomes, that may influence the information security culture deployment and development, emerged from the interviewees' responses and from the quantitative data obtained from the closed questions.

Table 5.2 provides a summary of the organisational values, practices and possible outcomes that may influence the information security culture in Case A. Each of the values is discussed in detail and illustrated with extracts from the case data below.

Management commitment:

The success of Case A's IT initiative was seen to rely to a large extent on consistent commitment from top management, and the associated outcomes including approval of IT's decisions and allocation of necessary resources. Notably, Case A key employees appear to share similar understanding and definition of information security management as reported in the literature ISO/IEC (2005). Also, this understanding seemed to be linked with the overall organisation's strategy development and the career paths of its employees, starting from the recruitment and hiring process and continuing throughout until the employee contract terminates. A majority of participants indicated that top management considers information security an important organisational priority (see Figure 5.4 (a)).

In turn, this level of commitment from top management (see Figure 5.4 (b)) seems



(a) Top management considers information security an important organisational priority

(b) Top management gives strong and consistent support to the security program

FIGURE 5.4: Influence of management commitment

to influence the middle managers'[2] commitment to stand behind the information security program. For example, the commitment of other department managers is clear as one participant [P6-A] noted:

> *"There has been a high level of commitment from top management, all department managers fully behind the program and its security."*

This level of commitment also appeared to facilitate an environment of collaboration among immediate managers, resulting in a consistent enforcement of information security rules and procedures by other managers.

Participant [P2-A] noted:

> *" the first step is management support that makes people work together and makes other managers support our [IT department] policy and enforce the related rules and procedures"*

Information systems structure:

Case A's Shared Services organisation provides shared services (e.g. administrative and IT) to all its business units, referred to as 'customers'. The aim of centralising the managerial services is to increase efficiency and efficient utilisation of available resources. The perceived benefits include an improved ability to share and efficiently process information, faster response to changes in technology and business needs, and reductions in costs because of economies of scale and resource sharing.

[2] In this current study, the terms middle, department and immediate manager are used interchangeably for managers who are not IT staff but are using and working with the information system on a daily basis.

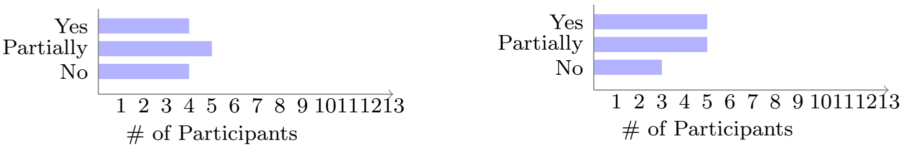
The IS structure was seen to contribute to the performance and effectiveness of information security management (according to Case A's annual report, 2006). In Case A, information technology resides within the ITS Group which is the seventh business unit in the organisation structure (see Figure 5.3).

Participant [P6-A] found this placement more productive because:

> *" this placement not only allows us to interact with our customers more efficiently, but also allows us to coordinate closely with related groups such as the HR people and other groups. I think we're seen as a service provider."*

The ITS group is responsible for providing leadership and management in the effective use of information technology infrastructure resources and supporting the IT needs of end users. The ITS Group handles IT standards, corporate IT projects and strategic IT plans. A relevant outcome of the standardisation of IT technology is that it has enabled ITS to improve the performance and effectiveness of the Information systems (Case A's annual report, 2006).

At the local level, responsibility for information security falls on the manager of the IT department in each business unit who is also charged with all other aspects of the information security system. Prior to this, each business unit's information technology department functioned independently. Each department had different platforms to work on with their chosen databases, network technologies, ERP systems and those built in-house (Case A's annual report, 2006).



(a) The organisation has a strong hierarchical structure

(b) IT staff are authorised to make important decisions related to information security issues

FIGURE 5.5: Influence of information security structure

Although, Case A seems to apply a decentralised approach, especially at the operational level, participants indicated that their organisation has a strong hierarchical structure (see Figure 5.5 (a))

The clarity of responsibility lines and coordination between the IT corporate, which is responsible for the enforcement of the information security standard, and the IT department, which has the responsibility to ensure that its members comply properly with implementing the standards, appeared to facilitate the role of immediate managers in Case A's information security management. The immediate managers' role was demonstrated through maintaining consistency in enforcement of information security rules and reporting information security issues directly to the IT department, for instance [P8-A]:

> *" we don't expect them [management people] to know everything about IT issues but we try to clarify things for them and let them know what their responsibility is... this helped us a lot and them in applying the IS policy and reporting our stuff...what I'm trying to say...it was impossible to achieve our objectives without their help... "*

In terms of decision style, almost half of the participants indicated that IT staff are authorised to make important decisions related to information security issues, while the other half indicated that IT staff are partially authorised (see Figure 5.5 (b)).

It can be seen from Case A's organisational chart, the responsibility for information security takes place at two distinct levels in the organisation structure. The first level is the corporate security program that creates standards and conducts oversight to ensure those standards are being followed. At this level, the information security program's placement in the corporate structure affects the way it is viewed by the organisation, and therefore its leadership's ability to manage the program and enhance the level of cooperation among department managers. Participant [P6-A] commented:

> *" Our position gives us [ITS group] flexibility to interact directly and closely with department managers."*

Skills and training:

In Case A, training programs are the responsibility of the ITS with direct involvement from the finance and human resource departments. In Case A, there is a specific budget allocated for information security awareness and training programs. The data from Case A revealed that information security activities related to training programs were seen to have a direct impact on the level of information security culture quality. As participant [P8-A] indicated:

> *" training programs are very important....and we have done quite well at the managers' level; but I think we need to do more at the users' level "*

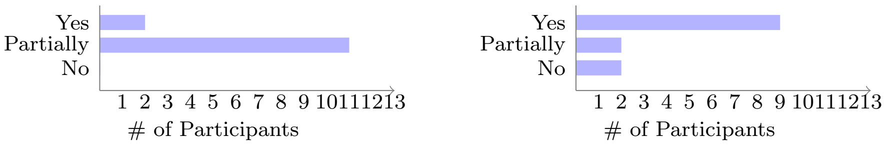
The cross tabulation analysis presented in Table 5.3 also indicates that the majority of the participants saw the lack of awareness and lack of training programs as the major obstacle to achieving improved security compliance.

TABLE 5.3: The top three obstacles to achieving improved security compliance in Case A

Participant	Lack of awareness and training programs	Lack of adequate technology	Clear direction in security procedures and roles	Lack of motivation programs
P1-IT	X		X	X
P2-IT	X		X	X
P3-IT	X		X	X
P4-IT	X		X	X
P5-IT	X		X	X
P6-ITM	X	X	X	
P7-ITS	X	X	X	
P8-ITS	X		X	X
P9-Non-IT	X	X	X	
P10-Non-IT	X		X	X
P11-Non-IT	X		X	X
P12-Non-IT	X	X		X
P13-Non-IT	X		X	X

The partially response in Figure 5.6 (a) indicates that training programs, in Case A, were limited to key managers and the staff of the IT department, who are expected to attend information security courses and seminars, where completion of the course is factored into performance evaluations. This limitation of training programs was reflected in the low level of information security culture among people at the lower level.

This challenge is further complicated where adequate in-house expertise was seen as a major challenge (see Figure 5.6 (b)).



a) There is a regular and structured training program to all members on information security

b) There is adequate in-house expertise for all supported services, mechanisms and technologies

Figure 5.6: Influence of skills & training

Awareness:

Case A relies heavily on their ITS, which has representatives at each of their business units' sites, to distribute information security related information to their employee base using different channels. For example, information security information is communicated to employees through an information security hotline, email notices, and the monthly Company General Committees meetings. Case A's sites are updated regularly with security information, and employees are encouraged to access these sites on a regular basis. When an information security issue arises, such as updating the information security policy or responding to a specific information security incident, these channels are utilised to communicate with employees, exchange valuable information, and identify best solutions. Participant [P4-A] pointed out:

> *" we [IT group] rely on our email system or the regular monthly Company General Committees meetings to pass on security awareness or any update about our issues"*

This focus on communication has its objectives. One example is to ensure information security messages are well communicated to all employees and to prevent deniability. One participant [P6-A] commented:

> *" we try hard to prevent deniability by providing all related information to our employees, so there are no excuses."*

However, the data revealed that there is no structured IS courses for all Case A's members as part of their education (see Figure 5.7(b)). This shortcoming may explain the participants' responses, in that, there is a perceived need for more awareness programs (see Figure 5.7(a)).

Case A's members, also, do not seem to take the routine information security awareness programs seriously. One participant [P13-A] commented on security warning emails:

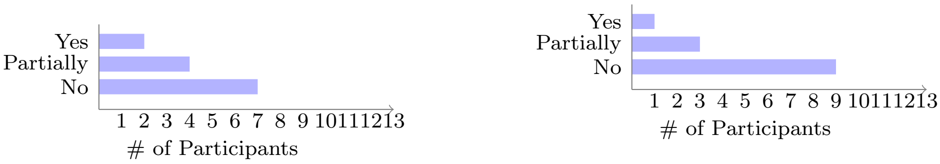
> *"the IT department sends a lot of warning e-mails related to security issues...almost every day...but I'm sure not everyone takes them seriously."*

Another participant [P9-A] admits that:

> *"Because some people have not enough time they delete warning e-mails without even bothering to look at them..."*

As can be seen from the cross tabulation analysis presented in Table 5.3, the main obstacle to information security compliance was cited as being the users and their lack of awareness. One participant's quote:

> *"The human factor is the main cause of information security incidents in our organisation. The major percentage of incidents are due to the disregarding of policy rules. The remaining incidents are due to technical faults in the system." [P5-A]*



a) There are appropriate awareness programs

b) organisation's members take IS courses as part of their education

FIGURE 5.7: Influence of awareness programs

Motivation:

In Case A, it appears that the Key Performance Indicators (KPIs) seem to play an important role in information security program implementation at the lower level. One participant commented:

> *"I think the overall organisation's KPI system helps in motivating people to comply with the rules " participant [P7-A]*

However, the case data revealed that the third most common barrier to achieving a high level of information security culture, that cited by Case A's participants, was the lack of motivation programs (see Table 5.3). This suggests that a specific motivation mechanism related to information security seems to help in encouraging employees to embrace information security objectives. One participant's quote:

> *"I think incentives that linked to information security can help to motivate people to comply with the information security rules " participant [P5-A]*

When participants of Case A were asked how tangible rewards (such as money and promotion) compare to intangible rewards (such as satisfaction and appreciation), they felt that the tangible motivation system achieved more positive results than the intangible system. Some of their responses:

> *"Tangible rewards are more effective." participant [P12-A]*

> *"It goes without question, tangible rewards"participant [P10-A].*

Information security management policies and standards:

Information security management standards seem to help in technology selection and security provisioning. Case A has adopted the International Information Security Management Standard ISO27002 and has been certified against it. Most participants were positive about the usefulness of the standard. For example:

> *" the ISM standard helps in technology selection and security hardening... not only for the IT staff but also for other staff" [P2-A].*

participant [P5-A]:

> "I think the information security management standard is useful in securing users' transactions by following the policies and guidelines."

participant [P3-A]:

> *"Yes. It [ISM Standard] clarifies the requirements and the way to comply"*

However, some practical issues related to the standards' implementation were raised by participants. One of the challenges in the implementation process is the shortage of IT staff that are technically competent with implementing information security standards. Interviewees reported a shortage of trained IT staff, particularly those who can adequately understand and can implement information security standards.

To quote a participant [P2-A]:

> *" we need people to understand them [standards] to execute them and also people to follow them."*

Participant [P6-A]:

> *"like any standards, information security standards need people who can fully implement them."*

This challenge is further complicated where training materials on the standards are only available in English and are not readily usable because of language barriers. Therefore, Case A had developed its own standard to establish its own level of security and to be complementary to the ISO standard. Participant [P6-A]:

> *“ as any standards, information security standards need people who can fully implement them.”*

> *“ ....information security standards some how are complicated and difficult to implement....so we translate some parts that are necessary to other departments.... and we also added some measures that are required by the industry... ”*

As an integral part of the information security management standard implementation, Case A has developed a contingency plan with a set of rules and procedures to systematically back up its information system. The system backups were maintained at an external site in another part of the country. This process is believed to ensure the availability of the information security system.

In general, interviewees indicated that their organisation's core culture values played a key role in the overall management process. Case A's mission statement stated that the organisation's core culture values include *“ providing quality products and services, and maintaining operational excellence while sustaining maximum value”*. It appears that Case A's information security program has capitalized on the quality principles of their culture to meet security objectives, specifically through the auditing process.

Case A conducts two forms of auditing to ensure that its information security program standards are being applied and followed. In addition to its internal audit teams, Case A uses third party auditors to conduct security-specific audits. Their goal in this process is to ensure that security issues are not overlooked by their internal auditors who are familiar with each department.

> *“ we here conduct two types of auditing to make sure that everything is going according to our standards and policy.... ”*

A relevant outcome of this audit process is to keep employees aware of information security responsibilities. According to one IT manager [P8-A]:

> *“ I would say that auditing makes people take security more seriously and also helps us to identify areas of vulnerability and weakness and correct them. ”*

Information security practices at the users’ level:

Participants were asked to select three main causes of security incidents at their organisation. The first main cause was cited as the users’ errors and non-compliance. One IT manager [P7-A] pointed out that users’ error remains the main cause of many of the information security incidents.

> *“all of the analyses we conducted on the various aspects of security incidents have identified carelessness and violation of policy rules as the main causes of accidents.”*

The second factor is more of a result of the first factor, that of viruses and malicious software. The third factor listed is hardware failure. This may reflect that there is a lack of information security staff or they might lack the required skills. Table 5.4 shows Case A’s participant responses.

TABLE 5.4: Top three main causes of security incidents in Case A

Participant	Viruses and malicious software	System or software errors	Cyber or internal based attacks	User errors or non compliance	System administrator’s errors or non compliance	Hardware failure
P1-IT	X			X		X
P2-IT	X	X	X			
P3-IT			X	X	X	
P4-IT	X			X		X
P5-IT	X			X		X
P6-ITM	X	X		X		
P7-ITS	X	X		X		
P8-ITS				X	X	X
P9-Non-IT	X			X		X
P10-Non-IT	X	X		X		
P11-Non-IT	X			X	X	
P12-Non-IT				X	X	X
P13-Non-IT	X			X		X

5.2.2 Summary of findings in Case A

The current analysis of the information security culture of members in Case A suggests that there was a high awareness of information security concepts and issues. The organisation to a high extent placed much importance on information security management aspects associated with both technical countermeasures (configuring, installing and maintaining various information technologies) and information security management aspects associated with adoption of information security policy, adoption of information security standards, adoption of awareness and training programs, and adoption of effective motivation mechanisms. Participants indicated that security related behaviors were mainly influenced more by top management support, by immediate managers in all departments, technical controls and management security initiatives. It seems that the lack of IT staff drive Case A to rely on a third party to manage and support a large portion of its information system.

The overall picture that emerged from this analysis is that Case A was maintaining a high level of information security culture that could be strengthened by focusing more on the users' level. Although, there was a comprehensive information security policy in place, it seems that there is a communication issue at the low level. This issue has negatively affected the users' level of compliance with information security rules and procedures. Further, where a violation of the information security related rules occurs, it is less likely that related rules are enforced. The motivation for complying with information security rules receives good attention among managers and individuals alike. The organisation's motivation system that is exemplified in the KPI mechanism seems to work well in the organisation.

In general, with respect to information security culture, Case A seems to maintain a proactive approach. This proactive approach was evident in much of Case A's information security related initiatives (contingency management plan, adoption of information security standards, and conducting audit process).

5.3 Case (B)

Three public organisations were approached for permission to conduct the study. These organisations have implemented successful IT initiatives in Saudi Arabia. There were concerns about the liabilities associated with formally documenting information security related issues. Also, gaining access to related organisations' information security documents is very time intensive to process. The geographical distance between the research activities and the case study organisations presented some logistical issues in terms of organising access to public organisations and implementing the data collection. In each case, the data collection is limited to interviews with managers and IT staff. Therefore, Case B is comprised of sixteen IT managers and staff from these three public organisations.

As mentioned before in Chapter 4, the unit of analysis in the current study, is the phenomenon itself (information security culture). The aim is to investigate and understand the information security culture, in light of the perceptions of IT managers and staff in different operating environments in the Saudi Arabia context. The author believes that these organisations are likely to have a similar approach to information systems security management. First, because the three organisations, to a large extent, operate under similar conditions and constraints. Second their approaches are constituted by the government's policy and regulation. Thus, grouping the three cases in one case will help in terms of analysing and reporting the case findings.

Table 5.5: Type and number of interviews conducted in Case B

Job position	Number of interviewees	Responsibilities of interviewees
IT department managers	6	Strategic policymaking in organisation, selecting information systems.
IT staff	7	Steering the IT implementation, providing support for end users, performing help-desk duties, maintaining functional and technical administration of the system and analysing ongoing use of the system.
Department managers	3	Working with the information system on a daily basis.
Total	16	

According to these organisations' Web sites, the objectives, vision, and missions of the IT department in these organisations are in line with that set by the Saudi Arabia Kingdom's strategy of using information and communications technologies (ICT) for continuous improvement by increasing the efficiency and productivity of the government's agencies. The organisations' published reports indicated that their efficiency and productivity were increased in apparent percentages as a result of the e-government services provided.

In each organisation, the IT departmental managers were in charge of managing their organisation's information system. The IT departments in each organisation are usually staffed by more than 35 employees all of whom were IT technical specialists. The IT departments at those organisations had to work with other public and private organisations that needed to interact with their systems. The IT department at each organisation and external consultants worked together on the development of the online services. A portal was launched for each organisation focusing on the following areas: (1) The organisations' administrative events; (2) Information products; (3) e-services; and (4) policy development and training. The focus today is to continue to expand online services to citizens and public and private organisations.

5.3.1 The influence of organisational culture values in Case B

In this section, the organisational culture values influencing the organisation members' beliefs and practices related to information security behaviour, in Case B, are presented.

Table 5.6 provides a summary of organisational values, practices and possible outcomes that may influence the information security culture of members in Case B, and their respective explanations. Each of the values is discussed in detail and illustrated with extracts from the case data below.

Management commitment:

During our interviews most of the participants stated that the IT initiatives at their organisations are successful because of the top management support (see Figure 5.8 (a)).

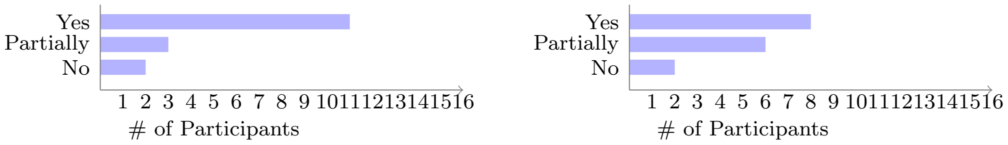
One participant [P3-B] noted:

> *"there has been a high level of commitment from top management, all department managers fully behind the program and its security."*

It appears that this strong commitment from top management helped in facilitating the IT department's mission by implementing and updating the right technology. One IT manager [P10-B] stated that:

> *"we have all the [management] support to adopt technical solutions if it can strengthen our information security"*

It also seems that the top management provided a strong support and foundation for the IT staff to take decisions related to information security at the operational level.



a) Top management considers information security an important organisational priority

b) Top management gives strong and consistent support to the security program

FIGURE 5.8: Influence of management commitment

One participant [P6-B] commented:

> *"we can't do what we did without their [top management] support, they value what we said and what we suggest.."*

Another quote from another participant [P3-B]:

> *"the top management already granted the authority to the IT staff to take a decision, of course within the organisational policy, rules, guidelines and procedures."*

Another reason participants feel that compliance to information security procedures and rules was evident relates to leadership. It was therefore very natural that one participant [P2-B] felt that information security culture started with the top management. He insisted:

> *"if the management team can be seen to be working hand-in-hand, everyone will follow suit."*

While the IT staff were pleased with top management strong support, top management has the final say regarding security related decisions, as one participant [P5-B] said during our interview:

> *"for sure, no one can take a decision unless he returns back to his top management and lets them be responsible for the action taken."*

However, a need for commitment from middle managers to back information security procedures and rules and provide direction was seen as crucial to information security culture improvement (see Figure 5.8 (b)). One participant commented [P6-B]:

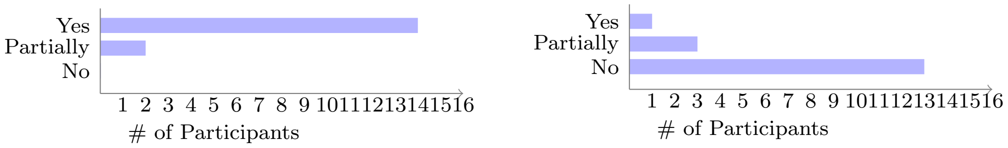
> *" I can say that the level of top management's support is good but we need more support and commitment from middle mangers to enforce our related procedures ..."*

Another participant commented:

> *" They [top management] can do more by directing middle managers to support our policy." [P11-B]*

Information systems structure:

In Case B, the IT departments are responsible for the comprehensive governance of organisation information security management, including organising, guiding, coordinating, monitoring and risk management, as well as formulating and fulfilling the information security management implementation. In Case B, it was seen that IS structure has a direct influence on the information security management effectiveness. As is common in public organisations, the functional and strongly hierarchical form of organisational structure appeared to be favored over other forms (see Figure 5.9 (a)). The main drawback of the functional hierarchy is that it is slow in decision making and has limited flexibility. Further, in a functional hierarchy, it appeared that information security is located at a low level, in the hierarchy, which is removed from the top management.



a) The organisation has a strong hierarchical structure

b) IT staff are authorised to make important decisions related to information security issues

Figure 5.9: Influence of ISS

In the context of decision style, a public organisation's preference for a strong hierarchical structure and consultative practice may indicate that IT staff are not authorised to make important decisions related to information security issues (see Figure 5.9 (b)). Also, the decision making process takes time and delays change. As one participant [P3-B] said:

> *" here things go slower than in the private sector and you need to cope with this kind of environment...."*

The perception of the middle managers in Case B, seems also to serve as an effective factor to encourage the employees as well as adjusting their potential resistance to the information security rules and procedures. For example, several participants brought out that individuals value and respond well to equal and consistent treatment by the immediate managers. As one participant [P11-B] put it:

> *" the rule has to be understood and to be applied to all people, then people will listen to their managers ."*

This suggests that middle managers' actions mediate the effect of their role on subsequent information security compliance behaviour.

In a related issue participants pointed out that collaborative activity is the base for creating a high level of information security culture. They distinguished between two forms of collaborative activity. The first form is the collaboration among middle managers and the IT department staff. This type of collaboration was seen as missing in cases related to enforcement of the information security rules and procedures. One IT staff member [P4-B] commented about the importance of the collaboration of middle managers:

> *" without department managers' understanding of our IT issues and willingness to apply the rules, there will be no such information security"*

The second form is between middle managers and their employees. In this regard, the process of making a group of people share the same vision about information security seems to be a very challenging task in organisation B. One manager's [P6-B] thoughts about enhancing information security culture were:

> *" to make all employees share the same level of awareness is a challenging task.... you have to be very close to your employees to understand their needs in order to pass your messages."*

In Case B, decisions are made top-down and reporting is made bottom-up. Information security management requires collaborative structures of decision-making, both within and across departments. This lack of required communication structure was a predominant topic for all participants in this case study. For example, one IT manager [P13-B] explained the difficulties of communicating bottom-up with respect to suggestions for improvement:

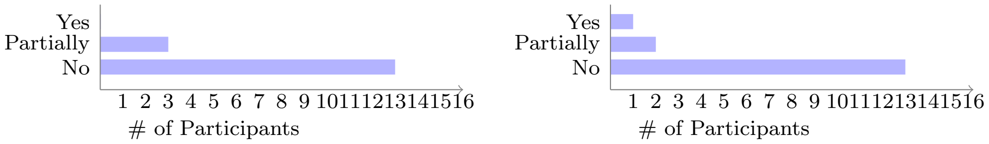
> *" It is a long process to communicate your ideas.... it takes the following road: from low level employees to their managers and then from managers to top management"*

It appears that a long process is a characteristic of a public organisation's management approach. For example, the IT department saw other department managers as slow in responding to their requests regarding manpower:

> *"for example, we asked for more people but things take time to be approved..." [P1-B]*

Skills and training:

The training programs are mainly targeted and designed for IT staff. In Case B, a shortage of IT skills clearly outweighed other factors in being attributable for slow development and deployment of information security culture (see Figure 5.10 (a) & (b)).



a) There is a regular and structured training program to all members on information security

b) There are adequate in-house expertise for all supported services, mechanisms and technologies

FIGURE 5.10: Influence of training and skills

This situation is also supported by comments from several participants:

> *"..I think we [IT department] must have structured training programs and enough IT staff to run these programs if we want to create an information security culture .... " [P3-B]*

> *".. shortages of IT staff is an issue and we [IT department] have to deal with this limitation on resources..so we rely on the private sector.... " [P13-B]*

> *".. we can't compete with the private sectors' incentives....shortages of IT staff will continue to be an issue in public organisations and we have to live with this limitation..... " [P2-B]*

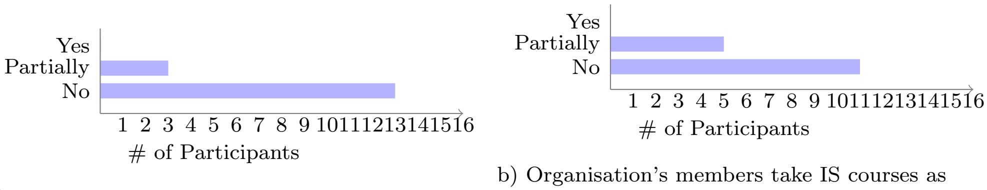
Awareness:

In order to emphasise compliance with information security rules and procedures and to ensure adherence to the organisations' rules, the organisations' policies in Case B consequently pay more attention to the employment contract. Besides this procedure organisations adopt some awareness activities related to information security. The users' awareness programs take the form of communicating e-mails, flyers and conducting related seminars. Those activities are accomplished by the IT departments cooperating with the human resources departments in the organisations. Participants attributed the success of their information security program to their early recognition of the benefits of implementing strong technical and management countermeasures, perceived by extensive awareness programs targeting middle managers. One manager stated that *"information security has been a priority from the beginning"*.

However, information security concerns seem to be an issue with departments that keep sensitive data about citizens and private organisations. There were some cases where individuals were not *adhering* to their organisation's rules. One manager [p14-B] remarked:

> *"when you have people working, expect mistakes".*

In general, participants indicated that raising security awareness was not given a priority in their organisations. Their responses indicated that low security awareness was a barrier to achieving improved compliance to information security (see Figure 5.11 (a) & (b)).



a) There are appropriate awareness programs

b) Organisation's members take IS courses as part of their education

Figure 5.11: Influence of awareness programs

Some participants also believe that information security management activities had not exerted a large influence on the users' security related behaviour. It was considered by participants that while the actual management activities were appropriate, their effectiveness was hindered by other organisational constraints, priorities, or cultural barriers. They perceived little change in users' levels of compliance related to information security as a result of IT management activities. Also, the influence of the related procedures was seen as a reaction to the incident. One participant [p7-B] explained:

> *"when we introduce new procedures that related to information security, we usually promote them to the users but users usually ignore them until an incident happens."*

This suggests that exposure to serious security threats will trigger the need for more related countermeasures along with enhancing previously existing mechanisms. Some participants also indicated less reliance on email based awareness. This is because adopting email in some public organisations as a formal medium has not been approved.

One participant [p7-B] explained:

> *" ...people here still rely heavily on paper more than our [ITC] system..."*

Further, participants realised that existing awareness activities were inadequate in raising a user's level of information security awareness to the level that it should be. Participant [P12-B] pointed out:

> *"..at the user's level more [awareness] is needed, but we have to deal with the resources we have.. " [P16-B]*

The same participant continued suggesting that appointing an employee who has an IT background as a liaison officer in each department between the IT department and the business unit can assist to deal with these issues:

> *"..you could have someone in each department who understands the procedures and can help those users on a daily basis" [P16-B]*

Motivation:

In Case B, it appears that no motivation mechanism related to information security was in place and it was taken for *granted* that individuals would follow the relevant procedures.

When asked about what motivates users to comply with an organisation's information security rules and procedures, most participants referred to management's actual practices as motivating the users' adherence or lack or adherence. In other words, they view the importance of compliance to be in line with the immediate manager's practices as a motivator. One participant [P3-B] stated the following:

> *"some managers are very strict, so their employees can't do anything but follow the rules. And some are flexible and take people for granted. This makes a difference to users' compliance "*

One of the IT team members [P2-B] also provided another insight about what motivates individuals to comply with the information security rules and procedures:

> *"To keep them secure of intruders, and any loss of their valuable information. For example, one of the employees didn't follow the policy of his company and did reformat his laptop, so he lost all his information. So what motivates employees to follow security rules and organisational*

> *procedures is the protection that they will have in making them more secure."*

When the participants of Case B were asked how tangible rewards (such as money and promotion) compare to intangible rewards (such as satisfaction and appreciation), they felt that the tangible motivation system achieved more positive results than the intangible system. Some of their responses:

> *"the tangible rewards come as the primary motive for the person to achieve, because all wish to increase their wealth, and money is the most important incentive given to the employee."[P16-B]*

The intangible rewards that come second place are where the employees is eager to achieve and attain respect. One participant's quote was:

> *"..intangible rewards comes in the second step."[P14-B]*

Information security management policies and standards:

According to the participants' perception and understanding, it appears that there was no specified information security policy in their organisation. However, the information security rules and procedures can be found in different documents. The related policies and procedures were properly designed and are well understood for controlling individuals' overall behaviour.

While Case B had not adopted any information security management standards, there was a positive perception about the importance of such standards. A sample quotation from a manager [P1-B] about the role played by information security standards in the organisation information security effectiveness was:

> *"Of course yes, managing your information security according to standards will give a base for you to build your information security more effectively."*

However, in Case B, organisations developed their *own standard* to establish their own level of security and to be compliant with government related policies. One participant [P4B] commented on this issue:

> *"we are a government organisation, we have to apply what government policies say"*

Information security practices at the users' level:

Reflecting on individuals' information security issues, the majority of participants believed that the users' own values and beliefs have influence on members' information security related behaviour. The cultural influences generated some information security issues behaviour that were not in accordance with information security rules and procedures. They were mainly centered on:

> *"password choosing in terms of authentication and downloading internet software. "[P10-B] .*

Participants were asked to select three main causes of information security incidents at their organisation. As can be seen from Table 5.7, the users' errors and non-compliance were the dominant factors that caused information security incidents. The majority of participants attributed this issue to the lack of clear directions and lack of related awareness programs. Some supportive quotes were:

> *"users don't follow information security related procedures because they are not aware of them..." [P5-B]*

> *"I think we need more awareness programs that are designed for all users.."*

> *" information security guidelines need to be communicated to all levels" [P9-B]*

The second factor,that of viruses and malicious software is more of a result of the first factor. The third factor listed is the system administrator's errors or non-compliance. This may reflect that there is a lack of information security staff or they might lack the required skills. Table 5.7 summarises Case B's participant responses.

In terms of the obstacles to achieving improved security compliance, the cross tabulation analysis presented in Table 5.8 indicates that the majority of the participants saw the lack of clear direction in security procedures and roles as the major obstacle.

5.3.2 Summary of findings in Case B

In summary, the information security culture of Case B's members was influenced by factors internal and external to the organisation. Top management support may influence members' levels of compliance directly through managerial security initiatives. This support may strengthen the IT department's position and thus may influence the security beliefs of other department managers in the organisation. An important external factor is that Case B has to comply with government related policies that may also influence the security beliefs of the employee. In general, participants view information security as a technical issue which is only the IT department's responsibility.

The overall picture that emerged from this analysis is that the organisations in Case B were maintaining a good level of information security that could be further strengthened. There was no comprehensive information security policy and it seems that it was taken for granted that individuals would comply with information security rules and procedures. In cases where a violation of the information security related rules occurs, it is less likely that related rules are enforced. The motivation for complying with information security rules receives low attention among managers of departments and individuals alike.

Table 5.6: Organisational values influencing the development of information security culture in Case B

Values	**Practices**	**Outcome**
Management commitment	Top management considers information security an important organisational priority. There was strong support for the IT department. Information security aligned to government's overall strategies. IT staff are authorised to take decisions related to information security at the operation level.	Facilitating the IT department mission by implementing and updating the right technology. High level of department managers' commitment to information security issues. Lack of regular support was seen to affect middle managers' level of support and enforcement of related procedures and rules. Level of co-ordination among departments related to information security rules enforcement needs to be strengthened.
Information Systems structure	Functional hierarchy form of organisational structure. Information security responsibility lies with IT department. No Information Security Officer has been assigned. Decisions are made top-down and reporting is made bottom-up. Decision style takes the form of consultative practice	Slow in decision making with limited flexibility. Unable to capture information security violations because of inability to cooperate. Collaboration was seen as missing in cases related to enforcement of the information security rules and procedures. It is more likely information security incidents go without discipline. Difficulties of communicating bottom-up with respect to suggestions for improvement
Skills and training	Information security training programs targeting only IT staff. Lack of IT skills. Reliance on third party.	Information security in the hands of third party. Confidentiality and availability might be compromised.
Awareness	Awareness programs take the form of communicating e-mails, flyers and conducting related seminars. Extensive awareness programs targeting middle managers. At the low level, individuals were taken for granted. No formal awareness programs. Awareness activities take a reactive perspective.	Users may lack understanding of the importance of information security and potential consequences of their security related actions. Low level of compliance to information security procedures and rules.
Motivations	No motivation mechanism in place and individuals were taken for granted. Highly depends on technical countermeasures.	Low level of compliance. Lack of co-ordination among departments and users. Low level of reporting security violations and sharing information/knowledge related to information security system.
ISM policies and standards	No adoption of related standards.Information security policy was embedded in the organisation's overall policies.	It seems that it was taken for granted that individuals would comply with information security rules and procedures. In cases where a violation of the information security related rules occurs, it is less likely that related rules are enforced.

TABLE 5.7: Top three main causes of security incidents in Case B

Participant	Viruses and malicious software	System or software errors	Cyber or internal based attacks	User errors or non compliance	System administrator's errors or non compliance	Hardware failure
P1-ITM	X			X		X
P2-ITM	X	X		X		
P3-ITM	X	X		X		
P4-ITM	X	X		X		
P5-ITM	X	X		X		
P6-ITM	X	X		X		
P7-IT			X	X	X	
P8-IT	X			X		X
P9-IT	X			X	X	
P10-IT	X			X	X	
P11-IT	X			X	X	
P12-IT	X			X	X	
P13-IT	X			X	X	
P14-Non-IT	X			X		X
P15-Non-IT			X	X	X	
P16-Non-IT			X	X	X	

TABLE 5.8: The top three obstacles to achieving improved security compliance in Case B

Participant	Lack of awareness and training programs	Lack of adequate technology	Clear direction in security procedures and roles	Lack of motivation programs
P1-ITM	X	X	X	
P2-ITM	X	X	X	
P3-ITM	X	X	X	
P4-ITM	X		X	X
P5-ITM	X		X	X
P6-ITM			X	X
P7-IT	X		X	X
P8-IT	X		X	X
P9-IT	X		X	X
P10-IT	X		X	X
P11-IT	X		X	X
P12-IT	X		X	X
P13-IT	X		X	X
P14-Non-IT	X		X	X
P15-Non-IT	X		X	X
P16-Non-IT	X		X	X

5.4 Case(C)

Case C is a non-profit organisation that provides support services for private organisations in Saudi Arabia. The main role of Case C is to represent the interests of its members to relevant authorities. It offers a wide range of services such as collection and dissemination of business information, identification of investment areas and opportunities, offering legal consultation, and development of labor resources. Case B employs over 3600 staff and has over twenty branches.

In Case C, the Information Center (IC) was set up to facilitate the collection of information required on time and with reasonable cost to its members. This was aided by the implementation of a document management system and mobile tools designed to improve knowledge dissemination and search and retrieval for managers and members. The IC department was staffed by 20 to 25 employees, amongst which there were 15 IT specialist employees.

Training activity at Case C is considered as one of its most important tasks: to develop the national workforce in several areas. The Training and Development Centre is responsible for the supervision and execution of this activity. Periodically, the Centre introduces a number of training services that vary according to training goals, types of trainees and their specialties and managerial positions.

Case C established their IT department to manage the organisation's new network which connects its headquarter to its branches and other public and private agencies. The IT department manager is in charge of managing the internal organisation's information system network. The IT department was staffed by 15 to 20 employees all of whom were IT technical specialists. Figure (5.12 provides the organisational chart of Case C[3].

A portal was launched focusing on the following areas: (1) the organisation administrative events; (2) information products supporting businesses in the state; (3)

[3] The organisational chart is a slightly modified version of the actual organisational structure in order to preserve confidentiality.

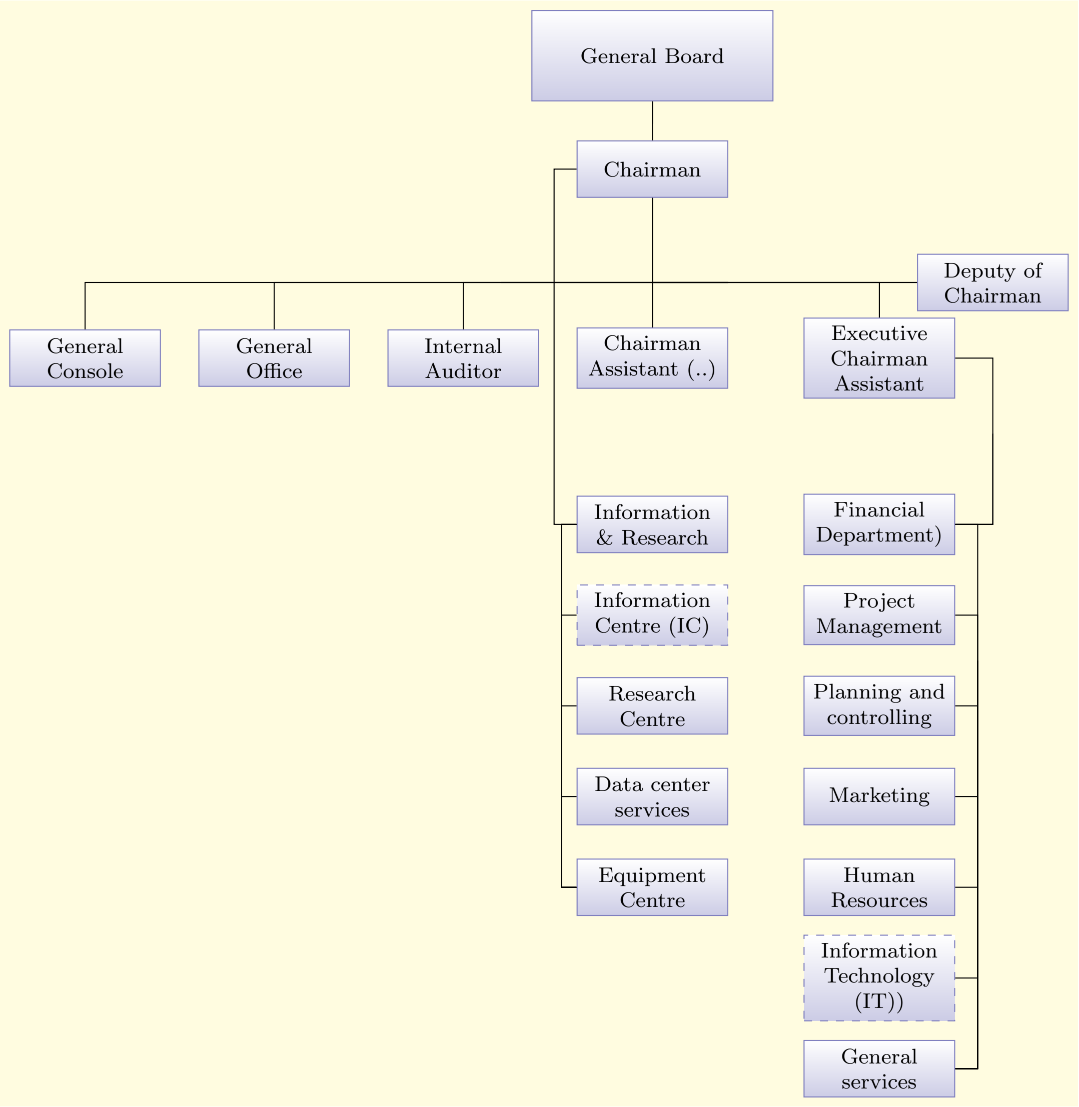


Figure 5.12: Case C's Organisational Chart

providing legal consultation and issuing permits; and (4) research and policy development on national business issues. The IT department and external consultants worked together on the development of the online services. Case C's members have access to high level networking events where they can discuss key issues and meet potential clients, suppliers, partners and competitors. The focus today is to continue expanding online applications to its members. Table 5.9 overviews the number of interviews conducted during this case study.

Table 5.9: Type and number of interviews conducted in Case C

Job position	Number of interviewees	Responsibilities of interviewees
IT department manager	2	Strategic policymaking in organisation, selecting information systems.
IT staff	6	Steering the IT implementation, providing support for end users, performing help-desk duties, maintaining functional and technical administration of the system and analysing ongoing use of the system.
Department managers	3	Working with the information system on a daily basis.
Total	11	

Table 5.10: Organisational values influencing the development of information security culture in Case C

Values	**Practices**	**Outcome**
Management commitment	Top management considers information security an important organisational priority. There was an allocation of resources to support its information security management at the initiation stage. No regular support to provide the required level of funding and resourcing. There was no indication that information security aligned to the organisation's overall strategies.	Low level of consistency enforcement of information security rules appears to be an issue. Lack of department managers' commitment to information security issues. Low level of co-ordination among departments.
Skills and training	No formal information security training programs. Reliance on third party. Outsourcing database maintenance.	Lack of IT skills. Information security is controlled by third party. Confidentiality and availability might be compromised.
Awareness	Individuals ware taken for granted. No formal awareness programs. Awareness activities take a reactive perspective.	Lack of understanding of the importance of information security and potential consequences of their security related actions. Low level of compliance to information security procedures and rules.
Information Systems structure	Internal fragmentation. Information security responsibility appears to be divided between two departments. No Information Security Officer has been assigned.	No individual department can be held accountable for the information security incidents that might occur within the organisation. Unable to capture information security violations because of an inability to cooperate. It is more likely information security incidents go without punishment.
Motivations	No tangible motivation. Highly depends on technical countermeasures.	Low level of compliance. Lack of co-ordination among departments and users.
ISM policies and standards	No adoption of related standards.Information security policy was embedded in the organisation's overall policies.	It seems that it was taken for granted that individuals would comply with information security rules and procedures. In cases where a violation of the information security related rules occurs, it is less likely that related rules are enforced.

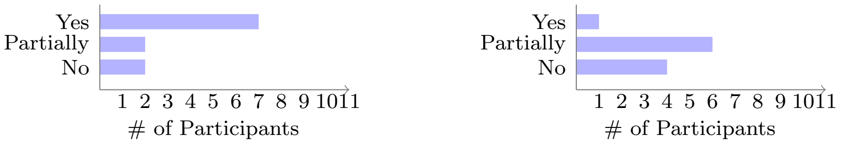
5.4.1 The influence of organisational culture values in Case C

In this section, the organisational culture values influencing the organisation members' beliefs and practices related to information security behaviour in Case C are presented.

Table 5.10 provides a summary of organisational values, practices and possible outcomes that may influence the information security culture of members in Case C, and the respective explanations.

Management commitment:

The data from Case C revealed that top management support was seen as a critical factor in the success of IT initiatives (see Figure 5.13 (a)).



a) Top management considers information security an important organisational priority

b) Top management gives strong and consistent support to the security program

FIGURE 5.13: Influence of management commitment

This support was expressed as appropriate funding and resourcing. However, it seems that this commitment from top management helped in facilitating the IT department's mission by implementing the right technology at the initiation stage of their program (see Figure 5.13 (b)). One IT manager stated:

> *" top management support was very important for us at the start of our program... and I think we need more from them to keep things running smoothly"*

The last portion of the above extract, seems to suggest that the level of management commitment did not translate into continuous actions to provide the required level of funding and resourcing in Case C. Another participant pointed out:

> *" they [top management] acknowledge the importance of the system security but it is hard to get financial support"*

The lack of resourcing and funding was seen as being due to the fact that non-profit organisations usually strive to keep costs of central administration low in proportion to costs to run programs.

> *" they [management] try to get the job done with less cost.."*

Participants from Case C also indicated the importance of all department managers' commitment and suggested that a strong directive from top management can assist in achieving such an understanding. One participant [P6-C]thought:

> *"managers have to do their part too... a strong push from top management can do the job."*

The sense of teamwork and cooperation across functions was not evident to most of the interviewees in the organisation. Reflecting on the lack of information security rules' enforcement, the IT department manager [P2-C] stated:

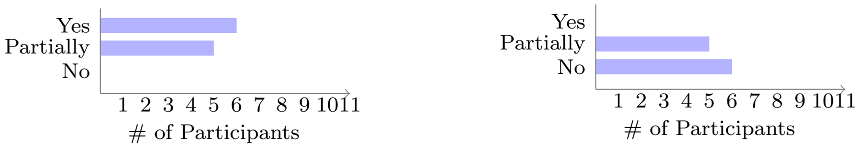
> *" it all goes back to cooperation and consistency and good communications...if you don't have this foundation, whatever the system you have will not work"*

Information systems structure:

In Case C, security of the information networks and the e-services falls under the IT manager, who reports to the Executive Chairman Assistant. The IT department is responsible for securing the network in which the e-services transactions take place.

On the other hand, the database security falls under the Information Centre (IC) responsibility, who, in turn, reports to the Directorate General for Research and

Information. The IC is responsible for securing the database and maintaining the organisation portal, which includes controlling and allocating the access control schema. In Case C, the IS structure was associated with difficulties experienced in managing the information security (see Figure 5.14).



a) The organisation has a strong hierarchical structure

b) IT staff are authorised to make important decisions related to information security issues

Figure 5.14: Influence of ISS

There was a concern that some overlap may exist between the responsibilities of the security of the information in the database server and those of the information security network and e-services transactions. Because neither of these responsibilities can be performed in isolation from the other, to secure the whole system requires a cooperative effort between the IC and the IT department. The IT department tries, at least, to draw the lines of responsibilities between their department and the IC department. They want to minimise any potential conflict by emphasising the bounds of security responsibility. Their manager [P1-C] explains:

> *" we all serve one goal, but when it comes to responsibility one should know his own boundaries,... and clearing this issue allows our staff to know their territory and avoid possible overlap of such responsibility. "*

This can be seen as an *internal fragmentation*. The issue of administrative fragmentation was illustrated by the fact that the responsibility for information security appears to be divided between the two departments. The result is that no individual department can be held accountable for the information security incidents that might occur within the organisation.

This tension between the two departments was further illustrated when the IC department hired an outside provider from the private sector to manage their database; an initiative that was rejected by the IT department. According to one IT participant [P2-C], their view was based on the point that:

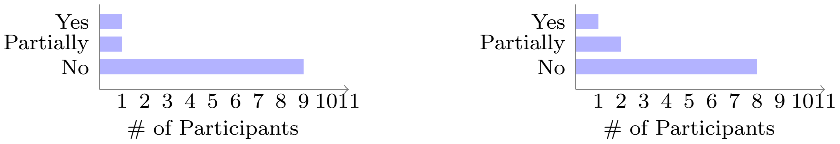
> *"we are against this move because it likely exposes our data to an outsider... "*

A related finding to the fragmentation issue was that Case C does not have a dedicated Information Security Officer. The IT manager is charged, among other IT activities, with the responsibility of information security management. The responsibility of the IT department ends with the installation and operation of the information system. After that it becomes the task of the users. One IT staffer explained [P9-C]:

> *"it is our job to connect the departments and maintain the system and it is the users' responsibility to use it properly... "*

Skills and training:

Among the various information security initiatives, Case C adopts some management activities such as training programs related to information security. This task is undertaken by the IT department cooperating with the human resources department in the organisation. The majority of participants indicated that there is a need for a structured training program aimed at all members (see Figure 5.15 (a)).



a) There is a regular and structured training program for all members on information security

b) There is adequate in-house expertise for all supported services, mechanisms and technologies

FIGURE 5.15: Influence of training and skills

Interviewees indicated that management activities related to information security, especially the training programs, are very important factors in achieving compliance to information security policies and procedures. A sample quote from a manager [P2-C] about the role played by management activities in their employees' security related behavior was:

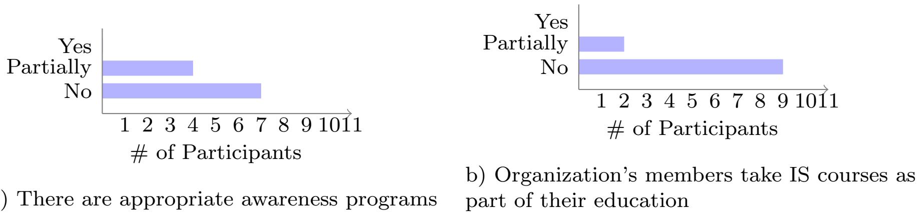
> *" most of the members lack relevant training and hardly follow any security policies. A training program can play a vital role in educating members of our organisation to adopt security guidelines."*

These initiatives were seen to suffer from the inadequacy of IT skills and resources (see Figure 5.15 (b)). One participant commented:

> *" information security management needs IT expertise to run the program, something that we lack..." [P2-C]*

Awareness:

The case data revealed that there were no formal awareness activities related to information security. Participants agreed that existing awareness activities were inadequate in raising information security awareness to the level that it should be (see Figure 5.16 (a) and (b)).



a) There are appropriate awareness programs

b) Organization's members take IS courses as part of their education

FIGURE 5.16: Influence of awareness programs

> *"although we don't have comprehensive security initiatives, some initiatives have impacted security related behavior such as awareness and training. There is a need to enhance the awareness of security issues and how crucial it is for our information security. "[P2-C]*

In Case C, the users' awareness programs take the form of communicating emails, flyers and conducting related seminars. Again, these initiatives were seen to suffer from the conflict between the two departments and the inadequacy of IT skills and resources.

> *"we all here try to keep costs very low" [P8-C]*

> *" more programs are needed, but awareness is not a priority in the overall budget " [P5-C]*

It seems that awareness programs are likely to have a highly priority when there is an incident. One participant commented:

> *" as the system is running no body cares about awareness...but when something wrong happens, every body talks about awareness " [P11-C]*

The above extracts indicate that awareness programs, in Case C, take a reactive approach rather than a proactive one.

Motivation:

In Case C, it seems there is no clear motivation mechanism related to information security being in place. The IT managers advised that the organisation has such a system which is linked to the overall motivation system but it seems that many employees are not aware of this mechanism:

> *"the motivation system is part of the overall system.....I think it is the role of all managers to motivate their people...."*

In contrast, almost every interviewee was aware of the punishment system and its details. When participants were asked if there were cases in which one or other of the systems was actually applied, the response was without any reference to such an eventuality.

At the user level participants suggested an additional strategy to make users adhere to the information security rules. They indicated that linking information security compliance to an employee's performance report would assist in improving the employee's security behavior.

One IT staff member [P3-C] commented:

> *" I think probably motivating people by linking users' security compliance to their performance reports would be a good approach. "*

Another participant's comment was:

> *" a good idea would be linking users' security compliance to one's performance evaluation report. "[P8-C]*

Information security management policies and standards:

At the time of the study, no comprehensive information security related standard or policy existed. However, the information security policy was embedded in the organisation's overall policies. There were also some documents, related mostly to technical aspects of information security management, scattered across several departments (IT, HR and IC). Respondents from organisation C emphasised the importance of organisational policies in information security development, for example, a policy to standardise managerial procedures. It appears that the lack of clarity about what kind of procedures to follow and enforce contributed to the lack of compliance with information security in Case C. One IT staff member [P7-C] explained:

> *" there are no clear procedures and guidelines related to information security issues and it is taken for granted that managers and individuals will do the right thing, but unfortunately, this is not always the case"*

Managers from different departments also supported the IT staff members' shared view that the absence of clear information security procedures and directions contributed significantly to most of the information security system incidents (see Table 5.12), although the IT manager [P1-C] made the following observation:

> *"they [the information security related procedures] have provided us with some guidance in different cases,initially. Now whether all departments would have followed and enforced them is another question"*

One participant [P9-C] also attested to the effectiveness of the information security policy:

> *" I believe that the information security policy will be effective because people will get a detailed understanding of the organisation policy...and determine what to do...in order to make it more efficient...and to have the different departments work together without conflict."*

From the organisation member's responses to our questions about the information security management issues, it appeared that this centered on the technical aspect of information security. This focuses on what technical solutions can be provided, and ignores the comprehensiveness of the information security management concept. This misunderstanding may have impact on realising the importance of information security standards. One of the IT staff members [P5-C] commented on the importance of information security standards in this way:

> *" last year one consultant company, which works as an information security auditor, came here with their product and gave a good presentation on the importance of information security standards. The management rejected their offer because they were not convinced of the urgency of such things ..."*

It seems that IT staff in Case C do not have the experience and background in information security management to value the information security management countermeasures. However, by depending on the technical countermeasures (antiviruses, firewalls, monitoring transactions), they have made some progress in their attempts to protect the organisation's information assets. In line with this view, interviewees pointed out that technology enforcement is an important factor leading the organisation's members to comply with the information security rules. A manager [P3-C] highlighted the role of technology power:

> *" we found it very effective in making people comply with the rules. Simply, if they want to download something from the Internet or don't choose a strong password the system will reject it."*

The importance of the technology role was echoed by another interviewee;

> *"there is a lot out there that the technology can do, but unfortunately we are lagging behind..."[P7-C]*

Information security practices at the users' level:

Participants were asked to select three main causes of security incidents in their organisation. The first main cause was cited as the user errors or non-compliance. One IT manager [P2-C] pointed out that user errors remained the main cause of many of the information security incidents:

> *" they [users] ignore the rules and think that it is our [IT department] job to fix the system and no one should question their behavior or actions... really this is what they think...so we just fix it and wait for the next one.."*

The second factor is more of a result of the first factor, that of viruses and malicious software. The third factor listed is the hardware failure. This may reflect the possibility that there is a lack of information security staff or staff might lack the required skills. Table 5.11 shows Case' C's participant responses.

In terms of the obstacles to achieving improved security compliance, the cross tabulation analysis presented in Table 5.12 indicates that the majority of the participants saw the lack of clear direction in security procedures and roles as the major obstacle. One participant's quote was:

Table 5.11: Top three main causes of security incidents in Case C

Participant	Viruses and malicious software	System or software errors	Cyber or internal based attacks	User errors or non compliance	System administrator's errors or non compliance	Hardware failure
P1-ITM	X			X		X
P2-ITM	X	X	X	X		
P3-IT			X	X	X	
P4-IT	X			X		X
P5-IT	X	X		X		
P6-IT	X	X		X		
P7-IT	X		X	X	X	
P8-IT	X		X	X	X	
P9-Non-IT	X			X		X
P10-Non-IT		X	X	X		
P11-Non-IT			X	X	X	

> *" there is no formal procedure in place to deal with member's resistance to security measures. We try to market security measures to middle managers as a contact point between us [IT department] and employees" [P1-C]*

Table 5.12: The top three obstacles to achieving improved security compliance in organisation C

Participant	Lack of awareness and training programs	Lack of adequate technology	Clear direction in security procedures and roles	Lack of motivation programs
P1-IT	X		X	X
P2-IT	X	X	X	
P3-IT	X	X	X	
P4-IT		X	X	X
P5-IT	X	X	X	
P6-IT	X	X	X	
P7-IT		X	X	X
P8-IT	X	X	X	
P9-Non-IT	X	X	X	
P10-Non-IT	X	X	X	
P11-Non-IT	X		X	X

The second most common barrier selected by Case C's participants was the lack of awareness and training programs. This is followed by the lack of motivation programs. When participants of Case C were asked how tangible rewards (such as money and promotion) compare to intangible rewards (such as satisfaction and appreciation), the tangible motivation system achieved more positive results than the intangible system. Some of their responses were:

> *"Satisfaction and appreciation, along with motivation, play a vital role in enhancing the security of the work environment. On the other hand, tangible rewards including money and promotion provide a big boost towards more security initiatives"[P11-C]*

When asked about any actions have been taken against individuals who were not complying with the organisation's information security rules, the answer gave no such references. This indicates that low enforcement appears to be an issue in Case C.

5.4.2 Summary of finding in Case C

The current analysis of information security culture of members in Case C presents a complex picture. It appears that there is a high awareness of information security issues. In Case C, the IT department placed high importance on security aspects associated with technical countermeasures (configuring, installing and maintaining various information technologies).

On the other hand, information security aspects associated with adoption of information security policy, adoption of information security standards, adoption of awareness and training programs, and adoption of effective motivation mechanisms were less emphasised. Participants indicated that security related behaviors mainly were influenced more by top management support and by immediate managers in all departments, and less by security initiatives. It seems that the lack of IT security staff plays a key role in the level of their information security quality.

5.5 The influence of national culture values in the three cases

The intention of the current study is to relate a range of cultural values and their potential effects on effective information security culture in the Saudi context. In this research the cases studied are in three Saudi Arabia organisations and the phenomenon of interest, unit of analysis, is information security management practices. In this section the discussion of the influence of the national cultural values in the three cases is combined. The reason for this is that members of the three cases belong to one national culture, as they operate in the same context, Saudi Arabia. Therefore, in order to determine which specific cultural values are important to the information security culture, the attributes of national culture attributes have been analysed by combining the participants' responses from all three cases. The national cultural items in the research framework were classified into four values using the national cultural model based on Hofstede (Hofstede,1984) and Hall's (Hall, 1975) values framework (refer to Chapter 4, section 4.2.2 - Figure 5.17).

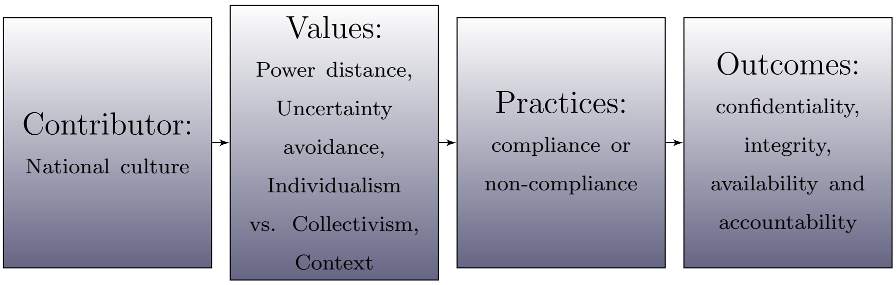

Contributor:
National culture
Values:
Power distance,
Uncertainty avoidance,
Individualism vs. Collectivism,
Context
Practices:
compliance or non-compliance
Outcomes:
confidentiality, integrity, availability and accountability

Figure 5.17: National cultural dimensions

The model assesses national culture along four values: (1) power distance, (2) uncertainty avoidance, (3) individualism vs. collectivism and (4) context. Table 5.13 provides a summary of national cultural values, practices and possible outcomes that may influence the information security culture of members in the three cases.

In general the interviewees raised the influence of cultural values as an important factor in information security culture development. Responses were coded to examine whether specific national cultural values were contributing to the information security culture development (for specific details of the interview data coding process see Appendix C). For instance, one participant mentioned the impact of an individual's cultural values:

> *"there are some people who carry with them certain cultural values that make it a little harder"[P8-C]*

which was coded as " cultural values have an impact on information security culture". Another participant commented:

> *"certain cultural values could make people do the right thing but others may not"[P6-A]*

This portion of the statement was coded as "cultural values may have positive or negative influences in employees' security behavior".

Most of the responses fell into this format where respondents indicated that there is a cultural influence on related security behavior which poses challenges, although managers overcome the challenges by extended exposure to managerial activities such as training and/or awareness. Additional examples include:

- One participant [P4-B] said,

  > *"cultural impact makes compliance to information security policy a challenging task. However, direct and face to face communication helps us get over that."*

- A manager [P13-A] mentioned:

  > *" I noticed that the cultural influences are very clear when dealing with new employees ...it takes sometime until they get familiar with all the organisation's related policies"*

- Another manager [P5-C] mentioned:

> *"employees' values play a major role in maintaining security-related behaviors"*

and he gave an example of,

> *"kindness and generosity"*

- Another participant [P1-A] added:

> *"culture plays into the initial phase, and different mentalities would judge such a thing from different points of view"*

Some respondents did not see all cultural values as a negative aspect, especially in the context of individual security related behavior. One participant [P6-C] summarised his thoughts in this way:

> *"there are different components of the culture values. Some of these values are good in promoting good behavior"*

He went on to illustrate his point using an example where some cultural values are useful in influencing individual security behavior:

> *" in some cases religious values dictate where one is going. These religious values may hold one from visiting prohibited sites which usually have some viruses or spyware that could cause security related problems."*

This indicates that some cultural values may impact information security in a positive way.

Additionally, some respondents did not find culture to be a major influence on individual security related behavior at all. Those were people who had been working in a relatively more western-oriented company and which has been an affiliate globally for a long time. Here are some of their responses:

One participant [P3-A] said:

> *"what matters most is the procedures....may be outside but not here [the organisation]."*

Another participant [P12-A] commented:

> *" I do not think so; it comes back to the level of enforcement.."*

5.5.1 National cultural values

In this section the national cultural values influencing the organisation members' beliefs and practices related to information security behaviour are presented.

Table 5.13 provides a summary of the national values, practices and possible outcomes that may influence the information security culture in the three cases. Each of the values is discussed in detail and illustrated with extracts from the three cases' data below.

Power distance:

The Power Distance value refers to the extent to which a society accepts the unequal distribution of power in the organization. Saudi Arabia scores high on this value, indicating that Saudi Arabia's employees are more likely to accept a hierarchical structure and the power of executives with higher ranking (Hofstede, 1994). In terms of information security management, power distance can have implications for how an organisation approaches information security issues. The influence of Power Distance can be understood by data collected about the actions taken in response to information security issues.

Two key issues of importance to information security were identified: **decision making style**, and the influence and **role of immediate manager**.

To investigate the possible influences of the power distance value on the decision making style, participants were asked to comment on the relationship between

Table 5.13: National cultural values influencing the development of information security culture in the three cases

Values	**Practices**	**Outcome**
Power Distance	At the senior-levels, in all cases there seems to be a higher level of equality among employees. Some information security decisions need to go through the hierarchy or top-level managers. Top management uses directive-consultative decision styles rather than more formal forms of participation or a delegation of authority.	May facilitate the IT Manager's preference to solve information security issues by reaching consensus with peers involved. IT staff involvement in the decision process is limited. IT staff are not always informed about all the changes and introduction of new projects related to the information system.
	At the lower level, employees usually rely on the managers to solve work issues.	Employees may not be involved in the decisions process, although they are the ones who raise the issues and execute the decision. More emphasis on the role of the immediate managers or work supervisors.
Uncertainty Avoidance	In general, most participants believed that they are risk averse. All cases take some kind of measured risk. Adoption of proven solutions, having contingency plans and conducting audit activities.	Immediate managers can be a factor leading some people to comply with information security rules.
	At the lower level, there is careless risk-taking (using shortcuts and downloading free Internet software). Resistance to information security measures is not an issue of concern. Reliance on the role of the technical enforcements and awareness.	Technical enforcements can be a factor leading some people to comply with information security rules.
Individualism vs. Collectivism	Sharing passwords is a security issue of concern. There are no formal mechanisms for sharing information and knowledge related to security. Information security knowledge sharing between technical staff takes informal approach instead. IT departments are satisfied with the level of cooperation from top management.	Immediate managers may have a tendency to not enforce the rules to punish their subordinates. Some employees may have a tendency as well to not report colleagues' violations. Some people may not willing to share information/knowledge with others.
Context	Miscommunication between members of the three cases at both levels. Communication takes face-to-face form. Exercising the informal open door policy. The contents of the policy are mainly related to technical issues of the system.	Members do not take the routine information security warning emails seriously. The message (e.g. information security policy) is communicated to a few selected people in the organization and little or no attention is given to the rest. Lack of guidance related to the information security issues. Employees may claim deniability of a specific rule or issue that has not been communicated properly to them.

managers and employees and the decision making processes that are associated with information security issues.

At the upper-level, in all cases there seems to be a sense of equality among employees, which facilitated the IT manager's preference for solving information security issues by reaching consensus with peers involved. This was supported by several comments made by managers and IT staff.

> *" after they evaluate the issue, they raise it to upper management for approval." [P3-A]*

Another quote from Case B:

> *"the IT department acts right away to solve any security issue, in case it needs something, then we go to the upper management for approval."[P7-B]*

A quote from Case C:

> *"when confronted with security issues, IT staff take suitable action for information security and sometimes ask for guidance and support from the management for taking initiatives."[P1-C]*

This indicates that the IT managers in this case would identify and analyse the issue, with all managers involved to inform, discuss and solve the issue together. Then the IT managers raise the issue to the upper management to get approval if needed. However, this level of engagement varies from case to case. Case A, for example, has appointed an Information Security Officer to ensure that information security issues are communicated to the highest level on a regular basis. It was seen that IT staff, in Case A, are empowered to make related decisions and they seem to have a higher level of authority for information security related decisions. For example, a quote from Case A:

> *"...the IT security team is fully empowered to make related decisions.."[P1-A]*

In both Cases B and C, it seems that some information security decisions needed to go through the hierarchy or through high-level managers. A possible foundation for this approval was the belief that upper management usually control what constitutes 'good and appropriate' information security management.

Although their involvement in the decision making process was limited, there were opportunities for taking some initiatives. For example, in Case B, some IT employees decided to write flyers and manuals related to information security for the organisation's users. One IT staff member[P3-B] said:

> *"..every one documents his part, it becomes like a manual for us.... from time to time we write security flyers and post them in each department poster, it is a kind of awareness message."*

In both Case B and C, to a different extent, it was clear that top management uses a *directive-consultative* decision style rather than more formal forms of participation or a delegation of authority. As one participant [P1-C] pointed out:

> *"... here the open environment approach allows people to communicate their issues with top management... it's the view of top management to remove the boundaries between our employees....but the final say usually comes from them [top management] "*

Although this process of consultation allows for a type of representation, in practice this informal open door policy tends to be very limited to a few selected people who are generally consulted. This limitation of this concept might explain the fact that in Cases B and C, IT staff were limited in their freedom to take decisions related to information security, and were led by the IT managers in taking any decision. For example, in Case B, IT staff were not always informed about all the changes and introduction of new projects related to the information system. The IT staff expressed that they lacked basic information and felt they were only informed about the managerial final decisions and did not participate in those discussions:

> *"...almost every six months we find a new product. I don't like it when you are just told to change to new products with not enough evaluations and you have to do this without your opinion being sought".[P2-B]*

However, at the lower level, the procedures are different. As is common for national cultures that score highly on the power distance value, executives and managers at an upper level are sought out for advice and guidance. In a high power distance culture, employees usually rely on the managers to solve work issues, since the managers often attain the role of a problem-solver. The impact of the power distance value is reflected in some of the information security managers' comments:

> *" when they face problems they come to me and I do my best.." [P2-A]*

> *"we direct them [employees]."*

IT staff report issues to the IT manager, who will provide guidance and directives, which are then implemented by the IT department. As one IT staff member [P8-C] commented:

> *"we follow the organisation's procedures by getting the decision from high management."[P8-C]*

These extracts suggest that people may lack problem solving knowledge and experience to approach their problems since managers handled all tasks in the absence of clearly related procedures. Under these conditions, employees may not be involved in the decision process, although they are the ones who raise the issues and execute the decision.

A related theme that could be attributed to the influence of power distance on information security culture is the importance of the role of the immediate managers or work supervisors. Some interviewees indicated that the manager's role, especially the immediate manager, is an important concern that influences employees' actions related to information security compliance. Some people chose to follow the rules although they did not have a strong supervision and directive from their managers. Hence it can be concluded that middle managers can be a factor leading some people to comply with information security rules. A sample quote from a participant about the role played by the immediate managers in achieving a good level of compliance is:

> *"the department manager's part is very important for us. Without their help, we can't have anything within our control. "[P4-A]*

> *" ...unfortunately, not every department manager is helpful in applying information security rules and procedures, there are some who really play a very good role and some just don't get it..."[P12-B]*

Another participant [P5-B] suggested:

> *"The security process can be enhanced by giving middle mangers more responsibility towards information security...."*

In summary, there was clear evidence that power distance seems to influence the decision making processes associated with information security issues. To a large extent the influence of the power distance value was more apparent in Cases B and C than in Case A. The rigid hierarchy, the limited level of involvement of IT staff and users in the decision process and their reliance on managers to solve work issues seems to reflect the influence of a high power distance culture.

Furthermore, the power of the immediate managers also seems to play an important role in individuals' behaviour related to information security, especially in Cases B and C.

Uncertainty avoidance:

Another value that determines organisational behavior is uncertainty avoidance, which refers to the ability of members within a national culture to deal with ambiguity. The level of uncertainty avoidance can provide an explanation about the level of risk-taking that certain organisations and its members can undertake in their actions in relation to information security issues and in relation to their willingness to change. Saudi Arabia scores highly on this value, indicating that Saudi Arabia society is uncomfortable with uncertainty and prefer predictability and stability (Hofstede, 1994). The fact that Saudi Arabia had a higher score on this value means that Saudi Arabia employees are generally not attuned to the notion of risks and also not willing to take risks.

Two key issues of importance to information security were identified as relevant to the uncertainty avoidance value: **risk avoiding** and **resistance to change** that are associated with information security issues.

To investigate the possible influences of this trait on information security management, participants were asked about risk-taking activities related to information security issues. In practice, uncertainty avoidance reflects a culture which needs rules and regulations ensuring certainty and security.

In general, most participants interviewed in all three cases believed that they were risk averse. The risk aversion may be explained by a very high organisational dependence on information systems.

One participant [P3-A] said:

> *" we all have the responsibility to maintain the organisation's information resources. I think no one will allow themselves to take any risk*

> *that could harm the system. If you lose a fraction of any information there is no way to get it back."*

This dependence also might explain the organisation's adoption of proven IT solutions, having contingency plans and conducting IT audit activities. The IT managers in Case A were also very keen on taking all possible measures to manage risks and not to leave things to chance.

One IT manager [P6-A]said:

> *" the IT security team is fully empowered to make appropriate decisions....they should adopt any solution that could strengthen the system's security...we don't want to leave things to chance....we have the support and we should use it for this cause"*

The risk aversion may also be explained by outsourcing part of the information security management. One participant [P7-C] commented:

> *"our department mostly depends on IT staff to get security issues resolved, but because we don't have the adequate resources we rely on a contractor to manage our data base.... at the end, it is our responsibility to make sure that the system runs with no problems...."*

When asked to describe how an IT department would approach a situation where the rules are not clear, or if there are no rules to govern decision making about information security, the response was:

> *" in the case of a new or unanticipated security situation, IT staff evaluate the situation and seek assistance from management to proceed if needed.."[P2-A]*

> *"the IT department evaluates the situation and takes the right action and seeks guidance from the management if needed."[P3-B]*

A quote from Case C was:

> *"when confronted with security issues, IT staff take the right action and sometimes ask for guidance and support from the management to proceed."[P1-C]*

These quotes may explain the broad view of the management with respect to the high level of maintenance of the technical infrastructure and day-to-day operations of information security technology. This also indicates that organisations' members in all cases appeared to take some kind of *measured risk*.

However, rapid changes in information security technology and new threats pose timely risks. The data indicates that the information security technology and related threats may pose a stronger influence on employees' intentions to take risks than the influence of this national cultural value. For example, there may be risks related to the choice of new technology or the adoption of new management solutions. To quote some participants:

> *"..the risk is that the organisation has to deal with IT new technology, new threats or new competitors.... it is part of any manager's job and he has to deal with it, of course, according to the organisation's policies"[P4-A]*

Another participant's stated:

> *".. recently we updated our system to 'the one platform system' and there were some challenging cases that could go wrong any moment; this was part of the risk that we have to deal with...." [P3-A]*

To quote one participant [P9-B]:

> *"..dealing with viruses or technical failure..... these are risks that we have to deal with almost on a daily basis."*

This indicates that IT staff make distinctions between two types of risk: unplanned risk which is imposed by unexpected security incidents (such as accidental breakdown of the IT system); and the planned risk associated with the dynamic nature of information security technology (e.g. upgrading the information system or adopting a new information security solution).

At the users' level, there is almost no risk-taking as all security related issues will be left to IT management. For example, in Case A, individuals have to complete an incident form and send it to the IT helpdesk or just inform their immediate managers, which is the standard practice in Cases B and C. Using incident forms in Case A was expected to provide information and feedback on department and employee information security incidents that help the IT management decision making process to feed into the measurement of an individual's performance system (KPI).

In Cases B and C, incident response approaches seemed to be slow and incomplete. This may translate into a negative impact (e.g. the incident goes without documentation, longer waiting periods before servicing, data unavailability and an individual's violation might go without discipline).

However, evidence was found of careless risk-taking by individuals who use shortcuts to accomplish some tasks or download free Internet software from the Web even though they are aware that such behavior may compromise the organisation's information system. One participant [P7-A] from Case A explained:

> *" ...in some cases employees' accounts are locked for any reasons such as exceeding attempts to access the system. When this happens to any employee they have to fill out a special form and send it to us to unlock his account...this process may take a long time...but we don't follow this literally..as soon as the staff member calls our help desk we do the job and they can fill the form in later on ...but some employees don't complete the form after getting their account unlocked.."*

The careless risk-taking issue was apparent in all cases as the following quotes from participants in Cases B and C indicated:

> *"even though we told them many times that downloading from the Internet sites is harmful to the system some users keep doing it…."[P8-B]*

> *"downloading free Internet software is an issue..." [P5-C]*

Besides risk-taking, **resistance to change** is another aspect of uncertainty avoidance which was observable. In general, information security rules and guidelines, seemed to be viewed in a negative way by the users, who may reject them or refuse to follow them, thereby preserving pre-existing norms and rules. Participants were asked to comment on resistance to information security measures. In almost all of the three cases participants' answers were in terms of *"I'm not aware of any"* or simply *"don't know"*.

This may indicate that resistance to information security measures is not an issue of concern in the three cases. However, some participants raised the importance of enforcing technical measures to deal with resistance to information security measures. The participants argued that the role of the technical enforcement and awareness helps users to understand consequences and potential punishments for their actions. Some of their thoughts were:

> *"technology based, there is no resistance.. " [P4-A]*

> *"awareness escalation and technical enforcements " [P5-A]*

> *"Any resistance to security measure action must be dealt with right away. Anyone violating the security policy should be punished based on his/ her action."[P3-B]*

A possible interpretation is that an organisation's procedures and information security policy may pose a stronger influence to an employee's intention to comply with information security measures than the influence of this national cultural values. This interpretation seems to be in line with the suggestions that organisational culture could override the influence of national cultural values. Another possible explanation is that the influences of certain national culture values may dominate the influence of others. In this case the value of power distance, presented in the role of the immediate managers, might have the upper hand in influencing an individual's intention to act against their manager's intentions.

To quote other participants:

> *" There is no formal procedure in place to deal with a member's resistance to security measures. We try to market security measures to middle managers as a contact point between us [IT department] and their employees." [P7-C]*

> *" such an issue [resistance to security measures] is left to immediate managers to deal with." [P13-B]*

In summary, at the management level, to a different extent, it seems that participants from the three cases believed that they were risk averse and complying with information security rules and procedures. On the other hand, the influence of uncertainty avoidance appears to have a limited influence on the security related behaviour of individuals at the lower level in all three cases. Furthermore, resistance to change, as another aspect of uncertainty avoidance, was not seen as an issue of concern in the three cases.

Individualism vs. collectivism:

The perceptions of and relations with one's colleagues in an organisation can vary greatly depending on whether the underlying national culture is individualist or collectivist. In an individualist society, the unit is each single person, and individuals together make up an organisation. In a collectivist society, the key unit is the company or organisation, which facilitates a more dominant environment for networking and inter-personal relationships.

Saudi Arabia scores high on collectivism and low on individualism, indicating that colleagues within the same company may view each other as members of an extended family (Hofstede, 2001).

This has implications for the information security in an organisation because this value might influence an individual's behaviour related to information security issues. Case data related to individualism vs. collectivism is presented in this section. Four key issues of importance to information security were identified which related to a high collectivism value: **the culture of sharing** (e.g. sharing of passwords and knowledge sharing), **cooperation**, **reporting** information security violations, and **willingness to enforce** information security related rules and procedures.

To start the analysis, information and knowledge sharing among members in the three cases is presented first.

Sharing passwords has been linked to the collectivism trait.

When participants were asked about the main causes of this issue, respondents considered *trust* among individuals and work pressure to be significant factors in the user's sharing behavior. Participants from the three cases indicated that they share their password with people they trust. The following quotes illustrate their thoughts:

> *"people share passwords because they trust each other...." [P6-C]*

> *" sometimes you have been asked to get a lot of work done right now, and you can't do it without help and they know that, so you have to seek help from your colleagues and you know who you share with." [P6-B]*

> *"simply because it is easy to do so and what matters is getting the job done.....as you get the job done no one will ask you did you share your password or not.." [P12-A]*

> *"some of our employees don't get the meaning and value of one's password, so they easily share it with their co-workers to get the job done."[P9-B]*

The above quotes indicated that sharing passwords seems to happen for reasons. Firstly, it seems that members were *not aware* about the importance of passwords with respect to information security. Secondly, sharing of passwords happened for a good cause which seems to be in this case *"to get the job done"*.

Besides sharing passwords, **sharing knowledge** is a second aspect that might once again be an indication of the influence of national cultures along the individualism and collectivism values.

The data from the three cases indicated that while there is a high level of awareness of the importance of sharing information and knowledge related to information security management, no evidence could be found of a formal mechanism that facilitates knowledge sharing between employees.

One participant proposed that the Internet usage and email policy, that is signed by every employee may contribute to the lack of knowledge sharing. The policy *prohibits* employees from engaging in online social networking and Internet blogging activities during work time.

> *"Sharing information happens only at the departmental level, but sharing information between users and IT staff.... I don't think it's a practice in our organisation nor culture. Usually, you share information with those you trust."[P10-A]*

One participant [P9-B] pointed out:

> *" management initiatives and cooperation can help to encourage people to share information that is related to information security effectiveness enhancement."*

> *"I can say that the open environment style allows for such thing but in its basic form...I mean it's not in a formal way.... Most of the solutions of related issues go without being documented.... " [P1-C]*

Another participant [P10-C] explained that some people are *not willing* to share information/knowledge with others:

> *"some people don't like to share with others how they solved a technical issue, because they want to keep their position... "*

However, information security knowledge sharing between technical staff happens informally after work interrelation. The conversation usually turns to work hours-related events whenever the group is together. They discuss issues and problems that they encountered in their daily work. As one participant explained:

> *"yes we discuss some issues in our lunch breaks or at the informal meetings. It is a good opportunity to ask for opinions or share some experience with colleagues... not only with IT people but with others as well, such as HR people..." [P13-A]*

This informal approach might not be sufficient to replace a formal process of sharing information. The same participant [P13-A] continued:

> *"...but you know after a while when you need it you have to remember who told you about such an experience.... "*

The employees who needed to share their knowledge or ideas seemed to be at a lower level of the organisational structure. As a participant [P15-B] put it:

> *"there are two things here, people who have the knowledge and are willing to share it, and people who don't have the knowledge and need it such as those at the users' level or new employees."*

One participant raised the importance of utilising *"a network of people and maintaining mailing lists of colleagues for sharing information security related knowledge"*.

These extracts may indicate the potential influence of the collectivism culture as a socio-technical factor concerning the improvement of knowledge sharing of topics related to information security.

Another issue related to the individualism vs. collectivism values is that of **cooperation** between individuals. The majority of participants stated that a quality information security culture relies on *collaboration* between all departments and between management and users from different areas, as well as on reaching an understanding of the importance of organisational information security.

It appears that the IT departments in all three cases were satisfied with the level of cooperation from top management:

> *"quality of cooperation is good with top management... anyone can directly communicate the issues or problems with the management..." [P1-C]*

The same participant explained:

> *"you are the expert and they value what you say..."[P16-B]*

However, the picture is quite different with respect to the level of cooperation at the user level:

> *"with users it's a little different because they are not educated about the importance of information security. They believe tech measures have the power to take care of any security threats...."[P11-C]*

Another issue that can be related to the collectivism value is that middle managers may have *a tendency not to enforce* rules to discipline their subordinates, an issue that was pointed out by more than one interviewee. One participant [P9-B] explained:

> *"some managers don't like to punish their employees.."*

When asked why he thought that, he explained:

> *"they don't want to be a cause of one's tragedy, and also they think that if they apply the rules they will not be likable"*

From a similar perspective some employees may have a tendency as well *not to report* colleagues' violations as they might view such action as characteristic of an unacceptable attitude that would negatively affect their relationship.

In summary, case data suggests that the collectivism cultural value is a strong attitude predictor of the effectiveness of information security management in the context of the quality of information security culture. To a different extent, the influence of a high collectivism value seems to play a key role in the following activities: the culture of sharing (sharing of passwords and knowledge sharing), cooperation, reporting information security violations, and lack of willingness to enforce information security related rules and procedures.

Context:

As in a high context society, communication is expected to be implicit among individuals. This might influence the flow and clarity of information (e.g. information security policy) among the organisation members. This influence seems to play a role in determining what information is transmitted, who receives it and the allowable circumstances under which different types of communication can be applied.

Saudi Arabia scores highly on this value. In a high context, society' members normally do not expect nor require much contextual information to be made explicit in the messages sent and received (Hall, 1976).

We analysed organisational members' **communication effectiveness** in this value by taking a closer look at their communication style - a concept that remains much discussed by both academics and practitioners as a key element in the effectiveness of information security compliance. While a clear majority of participants from all cases seemed to agree on the importance of communication in information security policy, their perspectives indicated that a lack of two-way communication between supervisors and employees is a major obstacle. The importance of communication of information security issues and the challenge associated with it is supported by participants' responses:

> *" it is of our interest that people understand the information security's procedures and rules..." [PB-A]*

> *"sometimes things go fast and you need to pass your messages as soon as possible to the users.... and more importantly people need to understand them correctly, this is sometimes hard to do..." [P3-A]*

When managers were asked to clarify, they pointed out that communication with users is an issue. One manager stated:

> *"communication between managers and employees needs more improvement in both directions" [P11-A]*

> *" Communication needs more improvement especially with users...the policy is there but they ask for directions"[P7-A]*

> *"Communication is an issue with users" [P13-A]*

On the other hand, low level staff think that their communication with top management is an issue and needs improvement. An example from one participant is:

> *" There is a lack of communication with the top management...they don't listen to what we say" [P11-C]*

> *" sometimes you have an idea or thought about a certain issue but when you think there is nobody going to listen, you just forget about it..." [P9-B]*

These two different views can be seen as a sign of miscommunication between members of the three cases at both levels. This aspect of high context may reflect the idea that individuals value the messages communicated *orally* or *face to face* more than the written ones.

Accordingly, we also asked participants about the relevance of different sources of information security related decisions. Oral and face to face communication were seen to be highly relevant by all participants in Cases B and C. The lack of an explicit form of communication in Cases B and C indicates that the communication at the users' level is most likely conducted in a face-to-face manner. This face-to-face approach was seen to have a significant impact on the effectiveness of the information security as the security policy is usually communicated in a written format to all users. The high context influence may also explain why most of an organisation's members *do not take* the routine information security warning emails *seriously.* As one participant [P13-A] commented on security warning emails:

> *"the IT department sends a lot of warning emails related to security issues ...almost every day...but I'm sure not everyone takes them seriously."*

In Case B and Case C, for example, the influence of the high context value may also be reflected by exercising the *informal open door policy* which tends to be *very limited to a few selected people* who are generally consulted. As a possible outcome of this process, the message would be communicated to a few selected people in the organisation and little or *no attention* given to the rest.

This last point can be clearly illustrated in the area of users' compliance to information security rules and procedures. In our interviews, members of both Cases B and C were not aware of the information security policy. There were no clear instructions provided for them by the IT department and system experts. The contents of the policy were mainly related to technical issues of the system. Users expressed their concern at the *lack of guidance* related to the information security issues such as *non compliance* to information security related procedures and *clarity of the responsibilities* of members of the organisation. One participant pointed out:

> *" ...people cannot work well without clear instructions or help. You have to have documented guidelines and instructions and to educate people about them as much as possible rather than taking people for granted, as occurred here. . "[P3-C]*

All participants indicted that emphasis on communication should be made to convey the importance of information security to their employees. This emphasis should generate a certain level of responsibility on an organisation's employees. This focus on communication also has its objectives as employees cannot *claim deniability* of a specific rule or issue that has been communicated to them several times through various channels. This is in line with one participant's comment on the importance of communications :

> *" ...we try hard to prevent deniability by providing all related information to our employees, so there are no excuses." [P5-A]*

To summarise, in accordance with Hall's framework, we can say that culture is to matter significantly. In the three cases, the high context value seems to influence individuals' compliance behavior related to information security rules and procedures. This attitude can be seen as a result of miscommunication caused by implicit communication between an organisations' members.

5.5.2 Summary of the influence of national cultural values in the three cases

The current analysis presented possible explanations regarding the influence of four national culture values on behavior related to information security culture in the three cases.

Overall, the analysis of the three cases revealed that some national cultural values may significantly influence the broad approaches that these three cases adopted towards information security management. These values acted to shape, to some degree, the processes and decisions related to information security management.

As a result, the findings appear to suggest that four national culture values: (1) power distance, (2) uncertainty avoidance, (3) individualism vs. collectivism and (4) context, were of relevance in that they seemed to play a role in shaping the way in which managers' and individuals' behavior and actions related to information security management.

5.6 Cross case analysis

In this section, the similarities and differences between the operational activities that support the existence and/or attainment of an information security culture performed by organisations and their members in all three cases are described in Section 5.6.1. Then, Section 5.6.2 provides details on the similarities and differences between the influences of national cultural values on the information security cultures in the three cases. Section 5.6.3 provides analysis of the information security practices at the users' level across the three cases.

5.6.1 The influence of organisational culture in the three cases

In this section the organisational culture values influencing the organisation members' beliefs and practices related to information security behaviour are presented. As discussed in Chapter 3, organisational culture values, that were generated from the related literature, were conceptualised in the research model to represent activities and factors related to information security culture deployment and development.

During our interviews information was obtained on the operational activities that support the existence and/or attainment of information security culture performed by organisations and their members in each of the case studies with regard to the top management commitment, the training program, awareness program, IT structure, appointment of information security managers, type of motivation system utilised, information security policy existence, and adoption of information security standards.

Table 5.14 provides a cross summary of the organisational values, practices and possible outcomes that may influence the information security culture in the three cases. Each of the values is discussed in detail below.

Table 5.14: Level of influence of the organisational culture values on the development of information security culture in the three cases

	Case A	**Case B**	**Case C**
Top management commitment	Top management considers information security an important organisational priority. There was an allocation of resources to support its information security management. Information security aligned to organisation's overall strategies.	Top management considers information security an important organisational priority. There was strong support for the IT department. Information security aligned to government's overall strategies. Extensive awareness programs targeting middle managers.	Top management considers information security an important organisational priority. There was an allocation of resources to support its information security management. However, there was no indication that information security aligned to organisation's overall strategies.
Training program and IT skills	Inadequate information security training programs. Reliance on third party (Low/medium)	Information security training programs targeting mainly IT staff. Reliance on third party (Medium/high)	No formal information security training programs. Reliance on third party (Medium/high). Outsourcing database maintenance.
Awareness program	There were formal awareness programs. Awareness activities take a proactive perspective.	Individuals were taken for granted. No formal awareness programs. Awareness activities take a reactive perspective.	No formal awareness programs. Awareness activities take a reactive perspective.
IT structure	-Well structured IT department. Information security responsibility lies in one department. -Officer of Information Security has been assigned.	Information security responsibility lies on IT department. -No Information Security Officer has been assigned.	Internal fragmentation, information security responsibility appears to be divided between two departments. -No Information Security Officer has been assigned.
Motivation	Adoption of KPI's approach as a motivation mechanism along with technical countermeasures.	Individuals were taken for granted. Highly dependent on technical countermeasures.	Individuals were taken for granted. Highly dependent on technical countermeasures.
Adoption of information security policy and standard	-A comprehensive information security management policy was implemented. -Adoption of the International Information Security Management Standard ISO27002 and certified against it. -Developed its own standard to establish its own level of security to be complementary to the ISO standard.	-Information security policy was embedded in the organisation's overall policies. -Has to comply with government's policies.	-Information security policy was embedded in the organisation's overall policies. -No adoption of related standards.
Change management	Conducts two forms of auditing to ensure that their information security program standards are being applied and followed. In addition to their internal audit teams, Case A uses third party auditors to conduct information security specific audits.	Conducts one form of auditing and actions would be taken to address an information security incident when it happened. Maintains a reactive approach rather than a proactive one.	Maintains a routine auditing activity usually related to routine procedures. Case C maintains a reactive approach to information security incidents.

Top management commitment:

In general, the findings obtained revealed that the three cases varied in their degree of comprehensiveness and integration of their information security management programs in part because of the different industry sectors that they were operating in. At the same time, all of them were holding the assumption that "the organisation's dependence on information systems is very high and security is an integral part of this equation".

To this end, all cases seemed to be successful in generating a high level of commitment from top management, to different degrees. In each case, for example, the top management commitment was exemplified by allocating the necessary resources and adopting the right technical solutions that were needed to support their information security programs.

However, the immediate managers' commitment to back up the organisation's information security program, in terms of consistency and enforcement of the related rules, was seen to have more influence on the development of the organisation's information security culture, than the top management commitment.

IT structure:

With respect to IT structure, in Case A, notwithstanding its adoption of the organisation's Share Services concept and participative approach, it was far more centrally determined. Corporate ITC, finance and human resources departments took a more direct and active role in the management of information security in all business units and departments, through the appointment of an Information Security Officer, the laying down of clear instructions and guidelines, and the implementation of organisation-wide information security policy and standard. This central control was, furthermore, supplemented by a number of mechanisms, including direct reporting relationships, the conducting of regular information security audits that fed into central information security plans which were held by corporate ITC, and training and development of awareness programs.

In both Case B and Case C a limited level of autonomy was given to IT managers. This autonomy was, however, constrained by the approval of upper management and by following organisation's rules and procedures. The reporting relationship between the IT departments and corporate HR was indirect and corporate HR did not take a direct and active role in the management of information security in the organisations.

Furthermore, Case B also exercised, as already noted, greater bureaucratic control through the slow process of decision making and the existence of indirect reporting relationships with the organisation's departments which encompassed a strong focus on ensuring that decisions were in accordance with government policies.

Training programs:

The case data revealed that training programs in the three cases have some form of information security training for their employees. However, these training programs were mainly designed for IT staff. Taking into account the different sectors within which the cases operated in both Case B and C, the reporting relationship between the IT departments and corporate human resources was indirect. Corporate human resources and related departments did not take a direct and active role in the management of information security in the organisations.

This last point can be clearly illustrated in the area of the lack of IT skills, even though that training was decentralised and they were free to choose the programs that suited them. Cases B and C showed awareness that they were lacking the skills and knowledge needed to support the e-solutions. In particular, their information security management process served to reinforce management's more general approach of adopting an incremental process. Thus, in Cases B and C the decision was made to hire a third party to manage a portion of their IT system. It also appeared that Cases B and C adopted a more gradual approach to information security management to partly reflect this concern.

Awareness programs:

In general, with respect to information security culture, both Cases B and C seemed to maintain *a reactive* approach rather than a *proactive* one. This reactive approach means that whenever the IT department countered with a behaviour that compromised or threatened IT security within the organisation, action would be taken to address that particular issue.

On the other hand, Case A relies heavily on their ITS, which has representatives at each of their business units' sites, to distribute information security related information to their employee base using different channels. However, the data revealed that there are no structured IS courses for all Case A's members as part of their education. This shortcoming may explain the participants' responses, in that, there is a need for more awareness programs.

Motivation mechanisms:

In terms of information security motivation mechanisms, in Case A, individual Performance Indicator (KPI) systems, as well as group bonus schemes linked to organisational performance, were established with the aim of motivating better information security compliance.

In both Cases B and C, the motivation for complying with information security rules receives low attention among managers' departments and individuals alike. Individuals in both cases seemed to be taken for granted and there was no reference to a specific motivation system.

Information security management policies and standards:

In both Case A and B, there was no comprehensive information security policy, and it seems that it was taken for granted that individuals would comply with information security rules and procedures. In cases where a violation of the information security related rules occurs, it is less likely that related rules are enforced.

In contrast, Case A was embracing a more global perspective in their information security management approach. Thus, Case A was operating with a background of international competition. This drove its management to adopt international performance standards, and implement standardised solutions and techniques to reduce costs and achieve financial and operational synergies. Case A adopted the International Information Security Management Standard ISO27002 and certified against it.

However, practical issues related to the standards implementation were raised by some participants. One of the basic challenges encountered in the practical implementation process is the shortage of IT staff that are technically competent in implementing information security standards. There is a shortage of trained IT staff particularly those who adequately understand and can implement information security standards. The challenge is further complicated where training materials on the standards are currently available in English and are not readily usable because of language barriers. Thus, in Case A, training and development was centralised in the hands of the Sharing Services unit with an aim to lessen its reliance on a third party.

5.6.2 The influence of national cultural values in the three cases

Analysis of the findings from the influence of the national cultural values on the information security culture in the three case studies revealed eight main areas of similarity and difference. These areas were decision making, compliance, risk-taking, sharing culture, collaboration, enforcement, reporting, and communication. These eight features of the findings appeared to reflect the influence of the four national cultural values (power distance, uncertainty avoidance, individualism vs. collectivism, and context).

In general, the findings obtained revealed that the four national cultural values appeared to exert a fundamental influence over the actions that had been taken by the organisations and their individuals in the three cases. However, as can be seen from Table 5.15, while the national cultural values appeared to have a fundamental influence on the three cases, variations of the degree of influence were found in each of these areas. It should be noted that the terms ‘high’, ‘medium’ and ‘low’ in Table 5.15, are used here in a ‘relative’ rather than ’absolute’ sense to draw out national culture values’ relative influence within the three cases.

TABLE 5.15: Level of influence of the national cultural values on the development of information security culture in the three cases

	Case A	**Case B**	**Case C**
Power Distance	Low	High	Medium/high
Uncertainty Avoidance	Low/medium	Medium/high	Medium/high
Individualism vs. Collectivism	Low/medium	High	High
Context	Low	High	High

In terms of the level of authority of the information security decisions, it seems that top management uses directive-consultative decision styles rather than more formal forms of participation or a delegation of authority. While, for example, IT staff were authorised to take information security decisions in both Cases B and C, a limited level of autonomy was given to their IT managers. This autonomy was, however, constrained by the approval of upper management and in following the organisation’s rules and procedures. However, in Case A, the IT security team seems to have a higher level of authority over information security related decisions.

A related theme that could be attributed to the influence of national culture (in terms of power distance value) on information security culture development is the importance of the role of the immediate managers or work supervisors. All three cases indicated that individuals intended to follow the expectations of management. They are more likely to approve actions that they perceive to be supported by middle managers and work supervisors which could have a significant influence on individuals' information security related behaviour.

In terms of beliefs about taking information security risks, most participants from the three cases were risk averse. This aversion is mainly attributed to the belief that taking risks could affect an organisation's information assets. In Case A, for example, risk aversion can be clearly illustrated in several activities related to information security management that have been implemented; for example, applying its own standards as a supplement to the international standard, conducting two types of audit activity (internal and external) and having contingency plans in place. In Cases B and C the risk aversion was clear in their management approaches, which tended to be more general, of adopting a gradual information security process in order to minimise the associated risk and in their relying on third party to manage part of their information systems.

However, at the users' level, there was careless risk-taking where individuals may use shortcuts, download internet software, and surf harmful Internet content. These practices varied among the three cases' members. While in both Cases B and C individuals' behaviour can be attributed, to a good extent, to the lack of existence and clarity of related rules and consequences of taking information security risks, in Case A, it was more of intentional non-compliant behaviour than a lack of existence and clarity of the related rules and consequences.

With respect to sharing culture, in all cases, sharing passwords was a security issue of concern. On the other hand, there was a positive perspective of sharing information security and knowledge in terms of both its importance and individuals' willingness to share. However, there were no formal mechanisms for sharing information and knowledge related to security. Sharing between technical staff took an informal approach instead.

A related feature of a collectivism trait is collaboration among organisations' actors. In Cases A and B, IT departments were more satisfied with the level of cooperation from top management than from the lower level and users. In Case

C, the low level of cooperation from both the middle managers and the users was reflected in the issue of a fragmentation of administrative responsibility, especially for information security.

Moreover, the collectivism trait influences can be clearly illustrated by a lack of enforcement of the related rules. In the case of B and C, middle managers may have a tendency to not enforce the rules to discipline their subordinates for sympathetic or protection concerns. In a similar vein, some employees may have a tendency to not report colleagues' violations for the sake of saving the group's image. In contrast, in Case A, it seems that the enforcement issue was minimised due to the adoption of the individual's key performance index (KPI) concept.

Finally, as in a high context society, communication is expected to be implicit among individuals. This might influence, as already noted, the flow and clarity of information (e.g. information security policy) among the organisations' members. This influence seems also to play a role in determining what information is transmitted, who receives it and the allowable circumstances under which different types of communication can be applied.

In Case B and Case C, for example, the influence of the high context value appeared to be reflected by exercising the informal open door policy which tends to be very limited to a few selected people who are generally consulted. As a possible outcome of this process, the message would be communicated to a few selected people in the organisation and little or no attention given to the rest.

This last point can be clearly illustrated in the area of users' compliance to information security rules and procedures. In our interviews, members of both Cases B and C were not aware of the information security policy. There were no clear instructions provided for them by the IT department and system experts. Furthermore, the contents of the policy were mainly related to technical aspects of the system. The users expressed their concern at the lack of guidance related to the information security issues.

In Case A, the influence of the high context value of cultural values was of less concern. It appeared that the prime factors that lessened the influence were the organisational structures and organisational cultural factors. The influence of these factors was compounded by several approaches to conveying its policies messages (e.g. reliance on middle managers, regular meetings, conducting audit activities, and utilising its email system).

5.6.3 Emergent findings:

Three related themes emerged from the three cases data.

- **Technology role:** The influence of information security technology to control individuals' information security related behaviour was seen to play a major role in shaping individuals' security related behaviours. Generally, while the three cases used information security technologies to control individuals' information security compliance, they differed with regard to the emphasis placed on them. For example, Case B and Case C both indicated that 'IT central control', through the mechanisms of the technology conveying and monitoring compliance, was their main method of control. In contrast, Case A placed relatively equal emphasis on technology controls and management aspects via standardisation, awareness, training, and motivations.

- **The immediate manager role:** The results indicate that the manager's role, especially the immediate manager, is an important concern that influences employees' action related to information security compliance. Hence we may conclude that immediate managers can be a factor leading some people to comply with information security rules. The positive significant relationship between immediate managers and the information security culture is consistent with previous research findings related to information security culture development (Ramachandran et al., 2008).

- **Change management:** In terms of the implementation of behavioural change strategies with a specific focus on information security, the previous analysis pointed to a number of different information management components. These include clear procedures and guidelines, decision support from top management, collaboration from all levels, well defined means of communication, adoption of motivation mechanisms and applying auditing processes. These components interacted with several factors such as adequate technology, training and skills. The objective of these practices was to influence and determine organisation members' courses of action. Thus, these management practices determined the actions of the employees to serve the interests of the organisation. This supports the idea that an organisation's rules and regulations have to be enforced and continuously monitored (von Solms and von Solms, 2004a). This was evident from Case A as well, where its information security program has capitalised on the quality principles of their organisational culture to meet security objectives, specifically through the auditing process. This audit process has proven to be a useful practice to keep employees aware of information security responsibilities and to assure compliance with information security rules and procedures.

5.6.4 Information security practices at the users' level in the three cases

In all three cases, participants were asked to identify three main causes of security incidents as well as the obstacles to achieving improved information security compliance in their organisation. The interview data from the three cases revealed that behavioural issues associated with users' security compliance behaviour were the most common concern. These issues include password sharing, using shortcuts, downloading Internet software, surfing potentially harmful content, ignoring relevant procedures, not sharing information and knowledge relevant to information security practices, not reporting security violations, and not enforcing security-related rules.

The first main cause of security incidents was cited as users' errors or non-compliance. One IT manager pointed out that user error was the main cause of many of the information security incidents:

> *"all of the analyses we conducted on the various aspects of security incidents have identified carelessness and violation of policy rules as the main causes of accidents."*

The second cause identified in all three cases may arise from the first and was identified as attacks from viruses and malicious software. In Cases A and C, the third factor identified was hardware failure, while in Case B the third factor was system administrator errors and non-compliance. This variation may reflect that both Cases A and C had issues relating to budget constraints. In other words, these organisations can not afford to implement effective security mechanisms and procedures to protect themselves or they have other more important budgetary priorities. Another possible explanation is that both cases were lacking information security staff or their current staff did not have the required level of skills. Whereas in Case B the issue seems to be more related to IT staff not following the right procedures and using shortcuts rather than lacking the required skills.

In terms of the obstacles to achieving improved security compliance, the cross-case analysis presented in Table 5.16 indicates that the participants in Cases B and C saw the lack of clear direction in security procedures and roles as the major obstacle. In Case A, the lack of awareness and training programs was identified as the first obstacle, while the lack of clear direction in security procedures and roles came as a second. This is followed by the lack of motivation programs as the third obstacle in all three cases.

The variation between the cases appears to indicate existence and implementation of an organisation-wide information security policy in Case A. Whereas in both cases B and C information security procedures and rules were embedded in other organisational policies. Nevertheless, in Case A, participants identified "lack of awareness" as the second obstacle which indicates that communicating the information security policy to users is an issue of concern in Case A. Table 5.16 shows the main causes of security incidents and obstacles to achieving improved security compliance in the three cases.

TABLE 5.16: The main causes of security incidents and obstacles to achieving improved security compliance in the three cases

	The main causes of security incidents	The obstacles to achieving improved security compliance
Case A	1)The users' errors or non-compliance. 2)Viruses and malicious software. 3)The hardware failure.	1)Lack of awareness and training programs. 2)Lack of clear direction in security procedures and roles. 3)The lack of motivation programs.
Case B	1)The users' errors or non-compliance. 2)Viruses and malicious software. 3)The system administrator's errors or non-compliance.	1)Lack of clear direction in security procedures and roles. 2)Lack of awareness and training programs. 3)The lack of motivation programs.
Case C	1)The users' errors or non-compliance. 2)Viruses and malicious software. 3)The hardware failure.	1)Lack of clear direction in security procedures and roles. 2)Lack of awareness and training programs. 3)The lack of motivation programs.

In order to build in-depth inferences from the case studies, further data analysis was conducted to identify patterns and relationships between individuals' information security related behaviours.

The results represented in Table 5.17 seem to suggest an emergent patterns of four modes of individuals' information security related behaviours. While there

Table 5.17: Modes of individuals' behaviour of information security culture in the three cases

Modes of individuals' behaviour	**Case A**	**Case B**	**Case C**
Mode(1)Not knowing-Not doing	Some IT staff were not sharing related information and knowledge because they were not aware of the right mechanism.	Most employees were not aware of the information security policy. There were no clear instructions provided for them by the IT department.	Most of the employees were not aware of the information security policy because there were no clear instructions provided for them by the IT department. Individuals' non-compliance behaviour was seen as a result of the lack of existence and clarity of related rules and consequences of taking information security risks.
Mode(2) Not knowing-Doing	Voluntary sharing culture of information and knowledge related to information security between IT staff.	As in public organisations, employees rely on the managers to solve work issues. Most non-compliance behaviour was prevented. Some national cultural values prevented users from visiting illegal Web contents. Sharing between technical staff takes an informal approach.	Sharing information and knowledge between technical staff takes an informal approach. Some cultural values dictated users actions.
Mode(3)Knowing-Not doing	Although users were aware of the information security procedures, some users intentionally showed non-compliant behaviours, for example; using shortcuts and downloading Internet software.	Employees were ignoring related procedures by downloading Internet software. Some employees may have a tendency not to report colleagues' violations for the sake of saving the group's image.	Users were using shortcuts and downloading Internet software. Some middle managers may have a tendency not to enforce the rules to discipline their subordinates for sympathetic or protection concerns.
Mode(4)Knowing-Doing	The level of information security culture indicated that the majority of members in all cases fit in this mode.		

were similarities in terms of all four modes of information security behaviour being present in the three cases, variations were found in the behaviours related to each of the modes.

Based on the current study findings from three case studies we placed each case on a grid chart (see Figure 5.18), as red, green and blue circles representing Case

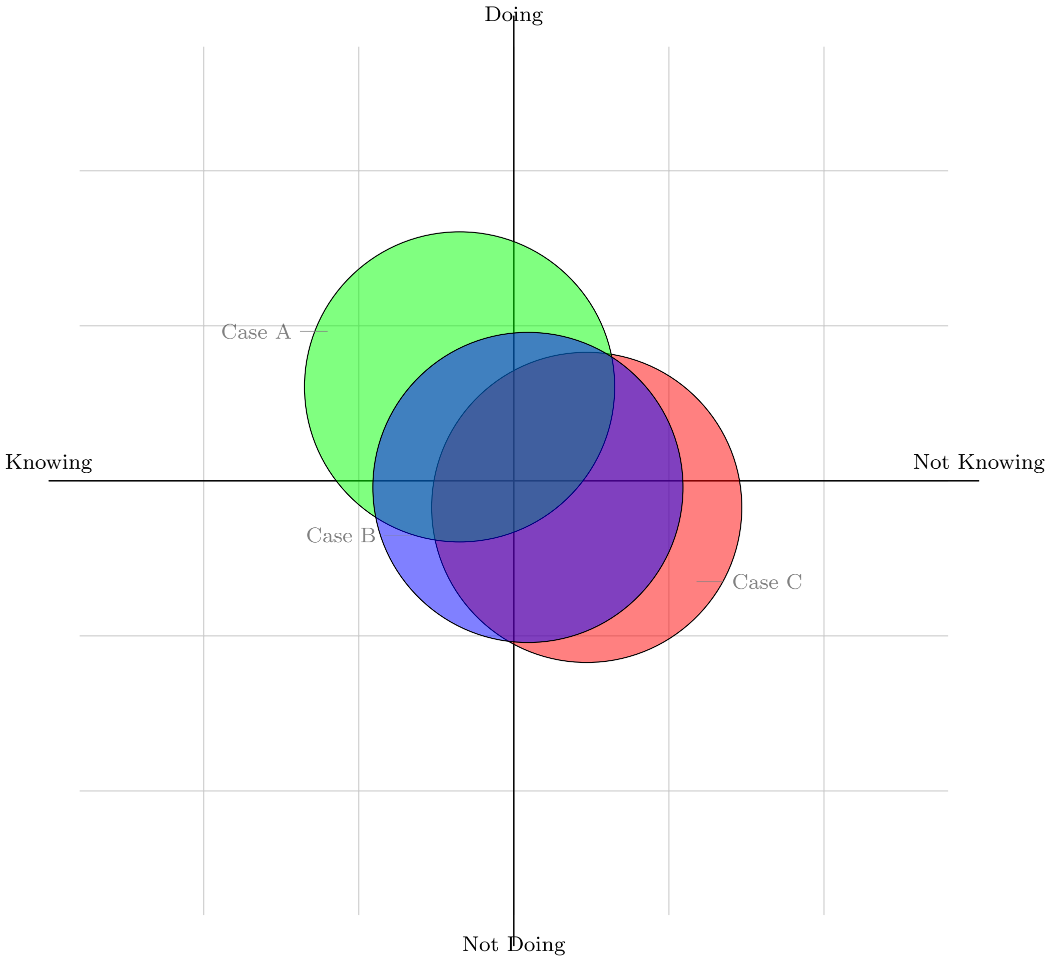


FIGURE 5.18: Information Security Behaviour Modes at the three cases

A, Case B and Case C respectively. The case study findings are reported below through an exploration of the four modes as follows.

Mode(1): Not Knowing-Not Doing Mode:

In Cases B and C, individuals were not aware of their organisations' information security policies; hence, they could not be expected to follow them. As noted earlier, regardless of having the necessary resources and the motivation to do so, if an individual lacks knowledge of the requirements or rules he/she may not exhibit appropriate information security behaviour. This is a type of cognitive failure that also includes issues such as misunderstanding the security policy or missing an update of the policy. In Cases B and C there was no evidence to show that unified and/ or clearly articulated information security policies had been communicated to users. The lack of understanding about policy appeared to be the main contributor to most of the non-compliance issues reported in Cases B and C.

For instance, respondents from both Cases B and C raised the importance of organisational policies to the development of information security (e.g. policy that seeks to standardise managerial procedure). It also appeared that the lack of clarity about what kind of procedures needed to be followed and enforced contributed to the lack of information security compliance in Case C.

One IT staff member explained:

> *" mostly it is taken for granted that individuals would do the right thing [following information security rules and procedures] but, unfortunately, individuals in most cases do the wrong things"[P5-C]*

Managers from different departments also supported the IT staff view that the absence of clear information security procedures and directions had contributed considerably to information security system incidents. All the interviewees in Case C indicated that they were not familiar with the information security policy, although the IT manager made the following observation:

> *"It [information security related procedures] has provided us with some guidance in different cases, initially. Now whether all departments would have followed and enforced them is another question" [P1-C]*

Mode(2): Not Knowing-Doing Mode:

The data collected from the case interview showed that most participants in three cases were risk averse which although they do not know predisposes them to act conservatively. This aversion was mainly attributed to the belief that taking risks could affect their organisation's information assets. In Case A, and to some extent, in Case B, a combination of self-consciousness as a member of the organisation and a willingness to abide by the organisation's rules indicated two aspects of both case's organisational cultures. The first aspect was a sensitivity to losing information, knowing that they will be questioned about it. The other was the hope for a reward, through the KPI systems, as well as group bonus schemes, which were linked to organisational performance in Case A.

In a similar vein, all participants pointed out that cultural values can influence employees' information security related behaviours. For example one participant noted:

> *"certain cultural values could make people do the right thing but other values may not" [P6-A]*

One can infer from the last part of this statement that certain individual cultural values may have a positive or negative influence on employees' security behaviour. Most of the case data appears to support this claim, for instance respondents indicated that there is a cultural influence on individuals' security-related behaviour which poses challenges, although managers may overcome these challenges by extended exposure to managerial activities such as training and/or awareness. However, some respondents did not see all personal cultural values as having a negative influence, especially in the context of individual security related behaviour. One manager summarised his thoughts in this way:

> *"There are different components of cultural values. Some of these values are good in promoting good behaviour." [P6-C]*

He went on to illustrate his point using an example showing that some cultural values are useful in positively influencing individual security behaviour:

> *" ...in some cases religious values dictate where one is going. These religious values may keep one from visiting prohibited sites which usually have some viruses or spyware that could cause security related problems."*

This data indicates that some cultural values may impact on an individual's security-related behaviour and ultimately influence information security culture in a positive way.

This last point can be further examined by understanding aspects of the relationship between managers and employees. As is common for national cultures such as Saudi Arabia that score highly on Hofstede's (1984) power distance value measure, executives and managers at upper levels are sought out for advice and guidance (Hofstede, 1984). In a high power distance culture, employees usually rely on managers to solve work issues, because managers often attain the role of problem-solver. The impact of the power distance value is reflected in some of the information security managers' comments:

> *" When they [employees] face problems they come to me and I do my best.."*

> *"We direct them [employees]."*

In these cultures IT staff report issues to the IT manager, who provides guidance and directives, which are then actioned by the IT department staff. As one IT staff member commented:

> *"We follow the organisation's procedures by getting the decision from high management."*

These comments suggest that people may lack the experience to resolve problems since managers deal with issues in the absence of explicit procedures. Under these conditions, undesirable employee information security behaviour and actions may be minimised as most activities have to be approved by immediate managers or work supervisors.

Although negatively affected by the lack of sharing and motivation mechanisms, some employees have adopted informal means for sharing information and knowledge related to information security systems. Members of Case A, for example, meet after work. The conversation usually turns to discussion of something that happened during their work hours. Whenever the group are together they discuss issues and problems encounter in their daily work. As one participant explained:

> *" Yes, we discuss some [ISM]issues in our lunch break or at the informal meetings. It is a good opportunity to ask for opinions or share some experience with colleagues.... Not only with IT people but with others as well, such as HR people.."*

Mode(3):Knowing-Not Doing Mode:

The data revealed that there was careless risk taking by individuals who used shortcuts, downloaded Internet software, and surfed harmful Internet content. These practices, as noted, varied between the three cases. In Cases B and C these behaviours can be mostly attributed to the lack of clarity about the rules and consequences of taking information security risks. Whereas in Case A, the data indicated intentional incidents relating to non-compliant behaviour. For example, Case A's Internet sites are updated regularly with security information, and employees are encouraged to access these sites on a regular basis. However, there was a perception that many of the organisation's members did not take these routine information security awareness programs seriously. One participant commented on security warning emails:

> *"the IT department sends a lot of warning emails related to security issues...almost every day...but I'm sure not everyone takes them seriously."*

Another participant admitted:

> *"Because some people do not have enough time they delete warning emails without even bothering to look at them..."*

Mode(4): Knowing-Doing Mode:

The level of information security culture in all three cases indicted that the majority of information security related behaviours fit into this mode. Data showed that members in all three cases believed that the organisation's dependence on information systems is "very high and security is an integral part of this equation". Most participants indicated that there was a certain level of comfort with the progress that their IT department was making in information security related areas. For example, in all cases, the data showed that top management commitment to information security was exemplified by allocating the necessary resources and adopting technical solutions to enhance information security programs.

The influence of national cultural traits (for example, Hofstede's power distance value) may be seen in the practices associated with this mode. Saudi Arabia is a high power distance society, and data from all three cases indicated that individuals intended to follow the expectations of management and they are more likely to approve actions that they perceive to be supported by middle managers and work supervisors. These traits appear to be having a substantial influence on individuals' information security related behaviour in all three case studies.

Furthermore, the data indicated that a combination of self-consciousness as a member of the organisation and a willingness to abide by the organisation's rules was present in the organisational culture of the three cases. The sensitivity of losing information, knowing that they will be questioned about it and the hope for rewards for reporting security incidents were also key factors in individuals' compliance with information security requirements.

However, as previously discussed, we should expect organisations' actors to keep their knowledge and skills current. It is not enough to secure the system by addressing the concerns of those who have the knowledge/skills to do the right things alone. Organisations are going through a rapid and costly change as they seek to adjust and perform in the changing environment (e.g. new regulations, new technology and new threats). Therefore, Mode 4 requires the same level of planning, monitoring and managing as the previous modes. An employee's behaviour may alter from one mode to another, depending on the organisational role the subject happens to be in, the state of technology deployment, and the relevance and availability of suitable training.

5.6.5 Summary of cross cases analysis

Overall, it is apparent that managers and members of all three cases are functionally interdependent, since they share a common task that cannot be reached by an individual alone. All three cases showed a high level of commitment towards their information security systems exemplified in allocating the necessary resources and adopting the right technical solutions that were needed to support their information security programs.

In general, the findings obtained revealed that in each of the three cases significant efforts had been made in order to maximise their information security culture. Moreover, the influence of organisational factors and management activities on the information security culture within the three cases appears to be relatively uniform. While there were inevitably differences of detail in their approaches, the nature of them was, as can be seen from Table 5.14, similar, notwithstanding the different sectors within which the cases operated.

As for the national cultural influences, generally, the findings obtained revealed that the four national cultural values appeared to exert a fundamental influence over the actions that had been taken by the organisations and their individuals in the three cases. However, as can be seen from Table 5.15, while the national cultural values appeared to have a fundamental influence on the three cases, variations of the degree of their influence were found in each of these areas. These variations can mainly be attributed to the variations of organisational efforts in each case and to the sectors that each case is operating in.

It was clear that national cultural values play a crucial role in all three cases' information security culture. However, a collective sentiment as exemplified by maintaining the information security management standards was adopted only by

Case A. This internal strength apparently facilitates the interaction with users and middle managers to attain a high level of information security culture.

5.7 Summary

This chapter presented the findings of the first part of case study protocol aimed at eliciting and synthesising current information security culture practices and values from public, private and non-profit organisations in the Saudi Arabia context. The chapter also presented the findings of the second part of the case study protocol aimed at identifying important processes and values that support the development and deployment of information security culture. A series of interviews with 40 participants from three organisations in Saudi Arabia was utilised to identify these processes and values. The respondents were mainly IT managers, information security managers, IT staff and department managers.

The three case studies demonstrate that technology, national and organisational values have a clear influence on management' and individual' information security related behaviour and practices, in return, influencing the development and deployment of information security culture in the three cases. The findings have not been reported in the information security management literature and this is a fruitful area for future research. The extant literature that analyses the findings will be discussed in the following chapter.

Chapter 6

DISCUSSION

This chapter discusses significant aspects of the findings and draws inferences in relation to successful information security management in organisations in the Saudi Arabia context.

The primary objective of the study, as stated in Chapter One, was to identify the influence of information security management values and practices on establishing a sound information security culture environment in organisations in the Saudi Arabia's context. The research explored information security management implementation: the national and organisational culture values in Saudi Arabia organisations and attempted to provide an understanding of the influence of these values on the development of information security culture.

In addition, one of the objectives of the study (see Section 1.4), was to make appropriate recommendations relating to successful development of information security management in Saudi Arabia's organisations. Hence, this chapter highlights the key findings and discusses their implications from the data analysis in Chapter Five as well as aspects from the literature review chapter. Then, an introduction to a proposed information security culture model emerging from the study findings will be presented.

6.1 Discussion on organisational culture values

Findings from the case studies indicated that when proper management activities are implemented they lead to the intended objective of information security management. Such activities included effective management commitment and leadership, awareness, procedures and rules and related standards, skills and training, and proper IS structure related to information security management.

The key findings related to the influencing organisational values are discussed below:

Top management commitment:

The literature suggested that obtaining top management's commitment is a necessary condition for an effective information security program (e.g. Ruighaver et al., 2007; Knapp Kenneth and Ford, 2006; Chia et al., 2002).

The current study suggests that top management commitment may have direct influence on the level of information security culture. This was through top management's willingness to exert the required effort, in terms of allocating the right resources and approving related decisions.

The current study, further, suggests that immediate managers' commitment to backing up the organisation's information security program, in terms of consistency and enforcement of the related rules, appeared to have more direct influence than the top management's commitment on the development and deployment of the organisation's information security culture. This is because of the direct interaction between the immediate managers and their employees.

This finding is also consistent with findings from the information system management literature (Ramachandran et al., 2008). Ramachandran et al. (2008) pointed to a limited effect of top management's influence on the level of interaction between organisations' members, as the influence is usually mediated by the mid-level managers.

IS structure:

The data suggested that the hierarchical level seems to be one of the most important factors in explaining differences in the level of organisations' information security culture. The level within the hierarchical was highly significant for most factors such as responsibility, process of relevant decision-making, communication and involvement of middle managers. This finding echoes several studies that pointed out the important impact of information system structure on the effectiveness of any information system project. The extent to which information systems are structured or dispersed throughout an organisation has an impact on the effectiveness of information security (Heeks, 1999).

This study investigated three different types of organisational structure. In general, the influence of the decision style was greater in public and nonprofit organisations than in private organisations. Both Cases B and C exercised, as already noted, greater bureaucratic control through the existence of a direct reporting relationship with IT managers, which encompassed a strong focus on ensuring that information security related decisions were approved by top management and were in accordance with the organisation's policy.

In contrast, in Case A, the responsibility lines were clearly drawn and IT staff were authorised to take more decisions related to information security management. The adoption of the organisation's Shared Services concept and participative approach, was far more centrally determined and effectiveness was further increased when corporate ITC, finance and human resources departments took a more direct and active role in the management of information security. It was also clear that certain management practices such as the use of goal-setting performance appraisals and individual performance-related mechanism limited the direct influence of top management over the information security effectiveness.

These findings are consistent with findings from the information system management literature (Rosacker and Olson, 2008; Caudle et al., 1991). Caudle et al. (1991) pointed out that in public sector organisations top management has a "politicised, larger external role than their counterparts in private firms". Hence, the direct influence of top management depends on the degree of the rigidness of the hierarchy, the delegated authority and level of interactions between top management and the organisations' members.

Furthermore, the data revealed that the appointment of an Information Security Officer, the laying down of clear instructions and responsibility, and the implementation of organisation-wide information security policies, supplemented by a number of mechanisms, including direct reporting relationships, was highly associated with the development of information security culture.

The relevant literature suggested that users should be held responsible for their actions. It means that if the users do not comply with the organisation's information security policies they will be held accountable for any negative results.

To assist in establishing a culture where users will accept that they are responsible for their actions, the data from the three cases suggested an additional element where middle managers and supervisors should also take responsibility for the information security issues.

Skills and training:

Previous studies have stressed that access to qualified personnel with the right skills, knowledge and capabilities is crucial for information security program success (Ho, 2002; Norris and Moon, 2005). Generally in developing countries, even when the need for security is recognised, management decisions are limited by the scarcity of funds and technical personnel (Khalfan and Ashawaf, 2003; **?**; Tarimo, 2006).

The current study identified that the shortage of IT staff that are technically competent in implementing information security standards is one of the basic challenges encountered in the practical implementation process in all cases under study. The current study also found that access to qualified personnel with the right skills, knowledge and capabilities is significantly and positively associated with the information security management principles and accordingly the organisations overall information security culture.

The shortage of trained IT staff particularly those who adequately understand and can implement information security standards was a major factor in leading the three case studied to outsource part of their information system. This finding is in line with Khalfan and Ashawaf's (2003) findings in that the shortage of trained IT staff was one of the key factors that seems to lead organisations in the Gulf region to outsource their IT systems.

The current study argues that while the outsourcing decision was justified by the related workforce deficiency, there were some concerns about the negative influence of this factor on the enhancement of information security culture in terms of both information confidentiality and availability principles in the long-term. The current study also suggests that certain management practices such as the creation of a partnership with Human Resources to better identify training needs, employee sensibility, recruitment and selection, and wages being linked to management by competencies, focusing on information security issues, appeared to have a direct influence on the enhancement and sustainability of an organisation's information security culture.

Awareness:

The development of information security culture development within organisations depends on all members' levels of awareness. Therefore, it is crucial to inform and educate them about the potential threats, the capability and limitation of available technological countermeasures and the relevant consequences of their behaviour. Relevant literature emphasises the importance of information security awareness among users. For instance, Siponen (2000a) indicates that information security awareness plays a crucial role in the effective interpretation and use of information system policies, procedures and technologies by the end-users.

The lack of security awareness was seen as a key factor in individuals' information security related behaviour in the three case studied. This study suggests that understanding the compliant mindset may be as equally important as providing information security awareness. The data from the three cases studied showed that some users were not exposed to information security awareness programs, but were willing to follow information security rules even when there was no one monitoring their behaviour.

On the other hand, some users had a sufficiently high awareness level, but admitted to departing from following the related rules and procedures. These findings suggest that while information security awareness programs are important, understanding users' underlying assumptions and beliefs could assist in designing the right program for each group to enhance the effectiveness of the information security culture.

Motivation:

The motivation to comply with information security rules and procedures is also of central interest to this study because understanding why and how this motivation occurs will help remove obstacles to achieving the desired quality of the information security culture. As discussed earlier, awareness alone does not guarantee greater willingness or a higher level of compliance. The results of this study indicate that an organisation's motivation system may increase people's loyalty and this may lead to more compliance with organisational rules and procedures.

The results also indicate an interesting relationship between people's perceptions of their behaviours and their actual behaviours in a couple of respects. First, the influence of the motivation system might positively impact members' security related behaviour but at the same time it might not assure prevention of negative security related behaviour. For example, data from the three cases have shown that some organisation members may not report information security incidents because there was no direct benefit to them from doing so.

Second, in the same fashion, the punishment system may prevent undesirable and negative security related behaviour but at the same time it might not lead to positive and unconscious security related behaviour. In other words, realising that engaging in certain behaviour could result in a severe punishment may work very well in preventing such behaviour but it may not necessarily encourage individuals to exhibit positive behaviour such as sharing important information or knowledge that could strengthen the organisation's overall system.

Thus, to achieve the efficiency and effectiveness of both systems, it is necessary to adopt them in a balanced fashion.

Information and knowledge sharing:

From an overall perspective, the study data suggests that there was a positive perspective of sharing information security and knowledge in terms of both its importance and the individuals' willingness to share. However, there were no formal mechanisms for sharing information and knowledge related to security and sharing between technical staff takes an informal approach instead. There was no organisational information and formal knowledge strategy in place to establish priorities for information and knowledge capture, nor for how it should be utilised. It was realised that while informal sharing existed, it also was limited to some technical knowledge between IT staff.

The observations from the case studies also pointed to a number of issues that appeared to affect the process of sharing information and knowledge in the three cases. For example, evidence from the three cases showed that some members were not willing to share information or knowledge with others. The provided explanation for this attitude was that some people were afraid of losing their power and position. This finding is consistent with the view that people may use knowledge as a source of power (Mohannak and Hutchings, 2007).

Further, the data from Case A have shown that some organisations' policies, such as the internet usage and email policy, may contribute to the lack of knowledge sharing. From the cases, we also observed that knowledge and information sharing is linked with trust and the existence of a formal mechanism for sharing information and knowledge. Hence, trust and formal mechanisms can be used to enrich an existing informal approach. There should be some form of mechanism to capture such information and knowledge related to information security in the organisation's information system. For example, with respect to sharing information, if one employee believes that someone's action is going to harm the organisations' information resources, this information should be propagated through the system right away to the right person in the right level. Similarly, if one employee believes that some knowledge is going to benefit the organisations' information system, this knowledge should be propagated through the system to the right repository and made available to the right people. These observations are in line with KM success models (Nelson, 2008; Jennex, 2006).

6.1.1 Summary of discussion on organisational values and practices

From an overall perspective, the study findings suggest that a number of organisational values and factors appeared to be interrelated. These inter-related factors included organisational culture values manifest in practices and activities related to information security management. The most important values and factors identified in this study were top management commitment, the level of training and IT skills, security awareness programs, organisational IT structures, the appointment of information security managers, type of motivation system utilised, existence of information security policy, and adoption of information security standards.

The study also revealed an important finding related to the effectiveness of organisational values and factors. The findings suggest that while information security management activities are important, understanding users' underlying assumptions and beliefs could assist in designing the right program and solutions for organisations' employees to enhance the effectiveness of the information security culture.

6.2 Discussion on national cultural values

Another main objective of the current study is to assess whether national culture values such as power distance, uncertainty avoidances, individualism vs. collectivism, and context have influence on the information security practices in different type of operating environments (public, non-profit, private organisations) in the Saudi Arabia context. The study data helped us confirm this influence. Further, the current study's analysis showed that the same set of values has a clear influence on management's and individuals' information security related behavior and practices across the three case studies.

Below is a highlight of the key findings relevant to national cultural values that appeared to influence the information security management effectiveness.

Power distance:

Power distance was identified in information security management mainly through understanding the course of action when security issues arise. In general, the study results indicated that, in all cases, at the upper-level, there seems to be a higher level of equality among employees, which facilitated the IT manager's preference to solve information security issues by reaching consensus with peers involved. This level of engagement varies from case to case.

The current study findings provided clear evidence relevant to power distance's influence on activities and practices related to information security management in the three cases. More specifically, findings showed clear evidence that power distance seems to influence the decision-making processes that is associated with information security issues. The influence of power distance was more apparent, to a large extent, in Cases B and C than in Case A. The limited level of involvement of IT staff and users in the decision process and their reliance on managers to solve work issues, seems to reflect the influence of a high power distance culture.

This limitation of involvement was evident from Case B's and Cases C's data, in that, IT staff were strictly limited in their freedom to take decisions related to information security, and were led by the IT managers in taking any decision. This also was evident at the top level, in both Case B and C, in which related decisions have to be approved by top management. This finding is in line with the view that participation in decision making is unlikely to be utilised in Arab organisations (Abbas, 1993; Bjerke and Al-Meer, 1993). The low level of employees' participation could be also due to the bureaucratic, rigidly hierarchical and governmental style, where managers and employees have to strictly comply with targets and orders coming down from the higher level, having very little room to exercise their own initiatives or style and little motivation to go beyond the assigned tasks.

Findings from Case A, however, revealed a different picture. IT staff, in Case A, were empowered to make related decisions. The appointment of an Information Security Officer also seemed to ensure that information security issues are communicated at a high level on a regular basis. This finding indicates that some forms of delegation in decision making are demonstrated by organisations' managers in the culture of Saudi Arabia, a country that is often referred to as scoring highly on power distance (Hofstede, 2001). This finding is in line with findings from the management decision making literature, with respect to the practice of authoritative as opposed to consultative decision styles in Saudi Arabia organisations (Al-Yahya, 2008). This result may signal a new pattern in managerial values and attitudes toward a more participatory culture.

In relation to information security, studies have long proposed that users' participation in decision making is associated with the effectiveness of information security culture (von Solms and von Solms, 2004b). The association between the users' participation and the effectiveness of information security culture was reflected on the users' motivation, role and task clarity, and the acceptance of and compliance with information security rules and procedures that users are expected to carry out. A logical conclusion in this regard, therefore, is that the lack of users' participation is likely to contribute to the lack of users compliance in the three cases studied, especially in Cases B and C.

Furthermore, an emerging factor that was identified is the power of immediate managers. The power of immediate managers seems to play an important role in individuals' behaviour related to information security, especially in cases B and C. The relationships with and perceptions of supervisors are important in high power distance cultures. Individuals intend to follow the expectations of management and they are more likely to approve a system that they perceive to be supported by top management (Karahanna et al., 1999). Thus, it is more likely that individuals accept the decisions and directions of their supervisors due to their superior position (Clugston et al., 2000).

The results indicate that a manager's role, especially the immediate manager, is an important concern that influences employees' actions related to information security compliance. Hence, it can be concluded that immediate managers can be a factor leading some people to comply with information security rules. The positive significant relationship between immediate managers and the information security culture is consistent with previous research findings related to information security culture development (Ramachandran et al., 2008). However, some people chose to follow the rules though they did not have a strong supervision and directive from their managers.

In light of the above findings, organisations' decision makers in Saudi Arabia should utilise the role of immediate managers and supervisors in fostering the development and deployment of their information security culture.

Individualism vs. collectivism:

As discussed earlier, the cross cultural literature maintains that Saudi Arabia' individuals score highly on collectivism and lowly on individualism, indicating that colleagues within the same company may view each others as members of an extended family (Hofstede, 2001). A clear manifestation in this research of the influence of the collectivism trait on information security practices is in the dominance of a culture of sharing, especially in relation to password sharing among members of the three cases organiasations. This phenomenon of password sharing can also be attributed to the inadequacy both of the awareness program and of the motivation mechanism. It is interesting to note that while sharing culture was negatively related to some information security principles (i.e. confidentiality and integrity) in public and nonprofit organisations, its influence among members of the private organisation was limited only to password sharing.

The results also indicated that the competitive setting of the private organisation may influence members and prevent them from engaging in collaborative activities and inappropriate information disclosures. Further, in the case of private organisation, the influence of the collective culture has probably been lessened by individualist influences, as the majority of employees had been working in a relatively more western-oriented company. Furthermore, the private organisation has had affiliation globally for a long time.

These results may suggest that individuals who exhibit a sharing culture, value close and group relationships, in that their sharing culture may lead them to participate productively in information and knowledge sharing initiatives. This group relationship view has been empirically supported by previous research indicating that a culture of sharing has a stronger impact on perceptions of collaborative activities in collectivist cultures than in individualistic cultures (Hasan and Ditsa, 1999). Hasan and Ditsa (1999) find that the collective nature of Arab society enhances the collaboration of team-based IT development because individuals are more willing to emphasise the common good of the project before their own advancement.

This contradictory result could be attributed to the fact that the individuals of Saudi Arabia do not necessarily rate highly on collectivism and lowly on individualism; instead, their sharing cultural tendencies may be situational and contingent on the magnitude of the task at stake. The results indicated that sharing password happened for a good cause which was, in this case, *"to get the job done"*. These findings seem to be consistent with Elashmawi (1993) insight about the Arab culture. Elashmawi pointed that Arab culture is neither collectivistic as in Asian society nor individualistic as in the western culture, yet strongly oriented towards maintaining family security.

An outcome relevant to the influence of the collectivism value is that immediate managers may have a tendency not to enforce the rules to punish their subordinates, an issue that was pointed out by more than one interviewee. From a similar perspective, some employees may have a tendency as well not to report colleagues' violations as they might view such action as unacceptable in that it would negatively affect their relationship. The study results indicated that such a tendency was found to be a major issue in public and non-private context while such a tendency was less influential in the private case. The national culture literature, indicates that when any cultural value is taken to the extreme, it produces a negative effect. When collectivism is extreme, people may value protecting others from perceived threats over other considerations. In this case, the tendency not to enforce related rules and not to report colleagues' violations might be perceived as containing threats to the group's survival.

Uncertainty avoidance:

The uncertainty avoidance value had a major impact on members of the three case studies in terms of managers' perceptions of issues related to information security. This suggests that a higher degree of uncertainty avoidance does influence members of the three case studies practices when it comes to their perceptions of information security issues -i.e. they do not have positive perceptions of risk taking related to information security management. For organisations' managers, they seemed to be more risk averse and this can be attributed to the basic underlying assumption that the organisations' dependence on information systems is very high. This might explain the organisations' adoption of proven solutions, having contingency plans and conducting audit activities. This is also reflected in why the IT managers in the three cases are very keen on taking all possible measures and not leaving things to chance.

In contrast, at the users' level, there was no significant positive effect of this value to avoid risk taking within the three case studies, suggesting that individuals who hold a high degree of uncertainty avoidance, may also exhibit risk taking in a different situation or position. At the users' level, the study results suggest that individuals' concerns about the consequences of actions may be less influential than their managers when thinking about risk-taking practices related to information security. This finding assumes greater importance given that Saudi Arabia's society is presumed to exhibit a high degree of uncertainty avoidance (Hofstede, 2001).

The current study, further, argues that this contradictory result may be attributed to the fact that Saudi Arabia's people may not necessarily be risk averse; instead, their uncertainty avoidance tendencies may be situational and contingent on the magnitude of the issue at stake. That is, individuals' risk taking tendencies may be activated, leading them to exhibit measured risk practices, when the organisation's interest is threatened. Otherwise, the intent to harm the organisation's information assets is not inherently assumed in their personal culture.

The findings also indicated that resistance to information security measures was not an issue of concern in the three cases. The data included instances where participants were asked to comment on resistance to information security measures. In almost all participants' answers in all three cases were phrased in terms of *"I'm not aware of any"* or simply *"I don't know"*.

A possible interpretation is that an organisation's procedures and information security policy may pose a stronger influence on an employee's intention to comply with information security measures than the influence of this national cultural value. This interpretation seems to be in line with the suggestions that organisational culture could override the influence of national cultural values. Another possible explanation is that the influences of certain national cultural values may dominate the influence of others. In this case the value of power distance, presented in the role of the immediate managers, might have the upper hand in influencing an individual's intention to act against their manager's will.

Context:

Last, in high context societies, communication is expected to be implicit among individuals. The high context score for Saudi Arabia showed a significant negative effect on the flow and clarity of information (e.g. information security policy) among the organisations' members. The effects of this value across the three case studies are interesting. Zakaria et al. (2003) pointed out that the influence of the high context value seems to play a role in "determining what information is transmitted, who receives it and the allowable circumstances under which different types of communication can be applied". The current study further argues that the case studies results indicate that the influence of the high context value may be reflected in the extent of the informal open door policy which tends to be limited to a few selected people who are generally consulted.

As a possible outcome of this process, the message would be communicated to a few selected people in the organisation and little or no attention was given to the rest. This last point can be clearly illustrated in the area of users' compliance to information security rules and procedures. In our interviews, members of both

Cases B and C were not aware of the information security policy, there were no clear instructions provided for them by the IT department and system experts. The contents of the policy were mainly related to technical issues of the system, and the users expressed their concern at the lack of guidance related to the information security issues such as what constitutes non compliance to information security related procedures and the lack of clear delineation of responsibilities of members of the organisation.

The study results provide further evidence of a 'two way communication gap' in relation to communication between management and users, especially in getting clarification from management, reporting violations of rules and regulations, and expressing opinions related to information security issues. IT managers indicated that the main causes for the communication gap were the lack of awareness and limited scope of training programs. Users perceive the communication style of top management to be below their expectations. This perception is acknowledged by IT managers, and they attribute it to having to deal with constant changes in information security technology in perceived threats and in rules and procedures and in the unsupportiveness of middle managers. Hence, it is important for organisations to broaden the awareness and training programs to include all users, to review the role of middle managers and allow for more involvement from the users side to narrow this communication's gap.

Similarly, the current study found evidence of an expectations gap concerning responsibilities related to enforcement and the kind of violations reporting that can be reasonably expected of middle managers. Although the IT department expects middle managers to perform such roles, managers are reluctant to do so since the relevant policies were silent on such roles. This gap may be attributed to the absence of relevant standards. In addition, the lack of IT staff who do not have competence to perform such roles, have affected the development of an information security culture. Thus, organisations should seriously consider introducing rules and regulations related to enforcement and violations reporting, as they are in high demand by both the IT department and middle managers.

An interesting point in this research is that "information security management standards" adoption could not be traced in our research results in the nonprofit and public organisations. This may be because of the low level of importance placed on standards in the studied organisations. In general, organisations in Saudi Arabia have only recently moved towards standardisation. Although some large organisations are required to apply standards and are considered as pioneers in Saudi Arabia, public and nonprofit organisations have not embarked on standardisation. The results in the current study point towards the view that in order to achieve efficiency and effectiveness of information security culture, all organisations in Saudi Arabia should move towards the adoption of information security management standards.

6.2.1 Summary of discussion on national values and practices

The current study revealed four points that indicate the way in which national cultural values have an influence on the development of information security culture.

The first is that power distance influence, in terms of the hierarchical power structures, appeared to limit operational staff involvement in information security related decisions. At the same time, the hierarchical power structures seemed to facilitate immediate managers and supervisors' role.

The second is that the influence of the uncertainty avoidance value was clear on individuals' practices at the upper management level. In contrast, at the users' level, there was no significant positive effect of this value on risk taking within the three case studies, suggesting that the cultural value of high uncertainty avoidance may be dependent on an individual's situation or position within an organisation. Further, an unexpected finding of this study, is that resistance to information security measures was not an issue of concern in the three cases.

The third related to the strong influence of collectivism value, encouraging sharing and discouraging enforcement and the reporting of security breaches. As a result, this produced a negative effect on individuals' information security related behaviour, thereby creating, what can be called, a " *chaos of patterns*". This may mean that individuals share sensitive information with others (internal or external) without any consideration to the value of such information. In many cases, this chaos seems also to participate in overriding the influence of many organisational and other national values in the three cases. This is in line with Levine and Moreland (1999) view, in that groups' influence tend to be more powerful in shaping individuals' beliefs than the broader organisational forces.

The fourth is that a high context value seems to influence the managerial communication style in the three cases. The influence of this value appeared to contribute to a 'two way communication gap' in the three cases studied.

6.3 Discussion of the emergent findings

The current study revealed three related themes that have emerged from the data in the three cases. These three themes have an effect on the development and deployment of information security culture. They are: the technological role, the immediate managers role and change management. Discussion on the influence of these emergent themes on the information security culture development and deployment is presented in this section:

6.3.1 Discussion on information security technology role

Traditionally the main information security services are the preservation of confidentiality, integrity and availability of information. Other properties such as authenticity, accountability, non-repudiation and reliability are also involved [ISO/IEC 27002:2005]. Relevant information security mechanisms, in the context of this study, refer to 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 organisations' information security system.

The significance of the current study's findings increases when it is noted that researchers in the area of information security culture have not considered technological measures as a crucial element in the development of information security culture. The analysed data suggested two aspects that could be linked to technological values. Firstly, the information security technology may have a crucial role in enhancing organisations' information security culture. To further clarify this point, the data of this study suggested that reliance on the effective control of technical countermeasures in the three cases was found to be very effective in shaping individuals' security behaviour. Examples of these countermeasures are forcing individuals to choose passwords of a proper length or preventing individuals from downloading or accessing certain web sites that may contain harmful threats. Hence, the reliance on automated controls provided through technical countermeasures and reliance on a third party consultant as opposed to the smaller role played by management initiatives, particularly, in the public and non-profit cases, is a logical way for overcoming the challenges imposed by the lack of in-house skills in order to establish a sound secure environment in all the three cases, to a different degrees.

Secondly, despite the perceived notion that a lack of technological solutions might negatively affect the level of information security effectiveness, the current study data suggested that, to a great extent, implementing the right technology was not an issue of concern in all three cases. The prevailing information management literature has identified the lack of necessary security technology as of major concern to many developing countries as it underlies efforts to establish access to the information age through effective ICTs (UN, 2005, Aljifri et al, 2003). This was not evidenced in the organisations we studied. Instead, gaining access to leading-edge technology was not an issue of concern in the three cases. A possible explanation for this finding is that management was more risk averse in this regard and also did not want to be blamed for not providing the support needed.

However, the issue is more of managing and maintaining the relevant technologies. From a strategic viewpoint, the lack of complete control over those technologies may cause some confidentiality and availability issues in the long run, for example, when the relevant licences and contracts are expired or terminated. This means that the total reliance on ad-hoc solutions and external providers versus an in-house approach needs to be thoroughly supported by an organisation that wants to sustain continued effectiveness of their information security programs.

6.3.2 The immediate manager's role

The role of immediate managers has been discussed under the influence of the top management commitment and the power distance in section 6.1 and 6.2.

In general, the results indicate that manager's role, especially the immediate manager, is an important concern that influences employees' actions related to information security compliance. Hence, the current study findings suggested that immediate managers can be a factor leading some people to comply with information security rules. The positive significant relationship between immediate managers and the information security culture is consistent with previous research findings related to information security culture development (Ramachandran et al., 2008).

6.3.3 Discussion on change management

Information security management by definition is an ongoing process. Change management, as a determinant of the success of information security development, was found to be of significant value. As threats increasingly evolve and technology changes the context within which that organisation operates will become more vulnerable to various threats. The introduction of new technologies and business practices may lead to integrations and transformations between various aspects of information related values, assumptions and behavior. An organisation that fails to maintain an effective presence in these reconfigured dimensions may find itself increasingly subject to severe threats from inside and outside.

Previous studies have shown a lack of formal change management processes, particularly when new information security rules and procedures are introduced to organisation members by the IT Department (Guha et al., 1997). The findings from the three case studies indicate that when organised change management support was provided, information security management proceeded with minimal resistance and generally on schedule. The current study findings also indicate that constant and productive collaboration between middle managers and users was a major factor in successful change management practice.

The current study's main argument is that change management strategy relevant to information security culture must consider an assessment of the observable aspects of the organisational culture as well as those which are related to national culture values. The current study is concerned with effective change management and behaviour change strategies relevant to information security practices such that they help in creating or optimising the organisation's information security culture to protect its information assets.

In terms of implementation of behaviour change strategies with a specific focus on information security, the previous analysis pointed to a number of different information management components. These include clear procedures and guidelines, decision support from top management, collaboration from all levels, well defined means of communication, adoption of motivation mechanisms and applying auditing processes. These components interact with several factors such as adequate technology, training and skills. The objective of these practices is to influence and determine the organisation members' course of action. Thus, these management practices determine the actions of the employees to serve the interests of the organisation. This supports the idea that the organisation's rules and regulations have to be enforced and continuously monitored (von Solms and von Solms, 2004a). This was evident from Case A as well, where its information security program has capitalised on the quality principles of their organisational culture to meet information security objectives, specifically through the auditing process. This audit process has proven to be a useful practice to keep employees aware of information security responsibilities and assure compliance with information security rules and procedures.

As the results indicated, most national values and attitudes can be attached to individual information security related behaviour. The influence of any values can impact the information security culture in a negative or positive way. For example, individualism is a value that belongs to some national cultures, which influences the sharing behaviour of people. When the managerial initiative is added, the information security related behaviour changes. The newly formed behaviour is now in a positive direction. The managerial initiative can also help an organisation to change its employees' behaviour to move away from sharing passwords and to move towards sharing knowledge and away from non-compliance towards compliance.

6.4 Summary of discussion on the values and practices

The findings of this study, indicated that management's and individuals' information security related behaviour have been influenced by the impact of organisational and national cultural values and the implementation of the associated technology.

The information security culture, in the three cases, has been developed in accordance with the available technology, its capability to adjust individuals behavior and the limitations of some country-specific factors in Saudi Arabia. Therefore, the relatively low level of compliance to information security rules and procedures, in the public and non-profit cases, was seen as a natural consequence of the absence of appreciating the importance of both information security management aspects and national cultural values on behaviour.

It is also possible that the studied organisations advance on certain aspects of some dimensions compensates for their shortcomings on other aspects of the same or different dimensions, especially if a given dimension in itself has a greater bearing on facilitating information security related behaviour than the remaining ones.

6.5 Implications of the findings

From an overall perspective, the study findings suggest that a number of factors appeared to be interrelated. These inter-related factors included national cultural values manifest in practices and activities related to information security management. The most important factors identified in this study were related to the influence of national culture on values in decision making, compliance, risk taking, sharing, collaboration, enforcement, reporting of non-compliance, and general communication. The current study findings from the three cases showed that some national cultural values are likely to have positive impacts on organisations' and individuals' behaviour in raising the information security culture quality. Hence, this facilitates the way to take practical steps towards a work environment that boosts information security culture and reduces negative impacts such as sharing passwords, disclosure of information and low level of users' participation.

The results also seemed to suggest that information security culture can be predicted from the influence of the organisational culture and technical countermeasures. In other words, the change in information security related behaviour seems to come directly from the change in organisational culture and technical countermeasures. In the three cases, and especially in Case A, individuals' attitudes have been changed by implementing more organisational and technical countermeasures. This implies that management should focus on the potential influence and features of individuals' cultural values to increase and sustain continued individuals' compliance.

Yet, this does not mean that controlling the influence of the organisational values automatically and completely overrides the influence and effect of national cultural values on the security related behaviour of the organisation's members. Rather, the influence of national cultural values and its effect on the members' security related behaviour and on the overall organisations' information security must not be neglected. This implies that the influence of national culture may remain silent or inactive and can be activated at any time, especially when the influence of organisational culture values or technical countermeasures are decreased (e.g. when decreasing the impact of the motivation system or missing a technical update).

When viewed in terms of the positive influence on information security related behaviour, it was also clear that organisational culture values and technical countermeasures have played the major role in information security culture formation. Thus technology and management initiatives were being utilised by means of access controls in organisations information systems. Hence the trend in the organisational structure of the studied organisations was towards a low level of compliance and the levels of risk taking and culture of sharing was significantly determined by the role of management related initiatives done through immediate managers' supervision and direction, and technological countermeasures. Examples of the latter are ad-hoc technology (antivirus, firewalls, intrusion detections and access controls schemes). These two measures are the dominant factors in the development of information security culture.

Consequently, the role played by information security management aspects in information security culture creation through adopting information security standards, contingency plans and policies was a relatively small one compared to technological countermeasures utilised in information security management in the public and non-profit cases. This fact is further indicated by the low rate of delegation of authority and low level of cooperation among top management and low level users.

The reliance on automated controls provided through technical countermeasures and reliance on third party consultants as compared with management initiatives and in-house skills for development of information security culture in these two cases, is a logical way for overcoming the challenges to establish a sound secure environment for these two cases. In Case A, the same mechanism is found to be enhanced by healthy cooperation between the middle managers and low level users with an active support from top management through real and productive commitment. However, this reliance is likely to encourage and cause long-term challenges as opposed to short-term challenges.

In light of the above, the level of information security culture generated from information security management initiatives can be more effective when they are implemented along with technical countermeasures to produce a sustainable long-term information security culture. Such a culture is caused by increasing interactions among decision-makers and organisations' members, socio-technical variables, policy instruments, guidance and adoption of relevant standards. These aspects need to be carried out in the spirit of participation among users, middle managers and top management. This finding allows us to contend that many of the factors that facilitate establishing an information security culture appeared to be the same factors that encourage trust, cooperation, and collaboration.

Another implication concerns the question of whether the organisational culture overrides the national culture, as opposed to the national culture overriding the organisational culture. The findings of the current study suggest that the influence of national culture may not have special formal properties that would set it apart from the influence of organisational culture values. Thus, we expect that the same subject might have been influenced by both national and organisational values. Therefore, the influence of national cultural values in some cases appeared to be overridden by those of the organisational culture and in other cases the other way around seems to hold true. This process depends on (i) how values are monitored, and (ii) how they are controlled. If the influences of national cultural values are identified by the management then their influences can be minimised by those of organisational or technical measures. This is exactly what the results suggested in Case A. Based on these findings, we expect two complimentary approaches for establishing an information security culture in an organisation: (i) the information security culture is created by help from managerial initiatives, and (ii) the information security culture is created by help from technical mechanisms. Thus, an information security culture can be created either by adopting new information security technical countermeasures or by help from the pre-existing organisational culture, or by both, as was seen in Case A.

The study findings revealed that too little attention was paid to positive cultural traits in their own right. This line of thought seems to suggest that attention should shift from just focusing on the negative aspects of the cultural values to include other values that may support in creating an effective information security culture. Organisations that are concerned about their information assets will surely be interested in minimising the influences of the negative aspect of national cultural values and maximising the influences of the positive aspect of national cultural values.

The successful information security management in Saudi Arabia should moderate the influence of these factors and even use them to enhance the opportunity for information security compliance. Managers' understanding of their own value systems and their appreciation and respect toward those of their employees will help to design appropriate management practices and thereby create an environment which fosters an information security culture.

From an organisational culture perspective, it was also seen from the case studies that elements of socio-technical interactions shaped individuals and organisations practices related to information security culture. For example, as examined in Case A, private organisations particularly faced with intense international competition, had to rapidly adapt to the radical changes in the external environment and to comply with international standards. As a result, specific organisational activities emerged that shaped information security related behaviour at both macro and micro levels.

Based on the cross case analysis, several main differences also emerge between public, non-profit and private organisations. It appears that while national culture values prevail in the public and non-profit organisations, organisational culture values seems to prevail in private organisations. However, in all three cases, utilisation of technical countermeasures is extensively applied. To a large extent, reliance on this approach was apparent in the case of both public and non-profit cases.

The findings further indicate that information security culture creation becomes more possible with training, awareness, and motivation playing a major role in shaping mental frameworks and creating a collaborative team. This is particularly important for individuals from organisations in developing countries, who wish to achieve and ensure an effective information security culture with the scarce resources.

Furthermore, one aspect that seems to be essential for a quality information security culture is to consider the natural trade-off created by two major concepts: scope and risk. The trade-off occurs because in general organisations ask employees to accomplish more things (scope) with less (risk). How management of the organisation solves the trade-off formed by these concepts seems to be a determinant of their success in achieving quality information security culture.

In light of this discussion, the current study proposes an information security culture model. This will be discussed further in the next section.

6.6 Towards an information security culture framework

An overview

From a theoretical point of view, information security culture is the product of socio-technical elements. Part of the social elements of information security culture is the internal cognitive structure of human beings. Cognitive structure includes "thoughts, beliefs, principles, attitudes, and habitual patterns of thinking". The cognitive structure helps individuals interpret, understand, and respond to the world around us. These social elements appeared to be difficult to manage, but the management activities and technological countermeasures that support the creation of information security culture can be the subject of management, in particular the activities, which involve all organisations' members and stakeholders and the information security systems infrastructure.

If the management is to develop methods to adjust individuals' security behaviour as a means of developing information security culture, it needs to understand the characteristics of both the factors that contribute to individuals' intentions and comprehension of the concept of information security culture. With respect to the former, the current research identified several values and factors related to cultural values both national and organisational and technological values. Each of these values may contribute either negatively or positively to the intention of individuals' information security behaviour. With respect to the later, the current literature indicates that researchers were hesitant to provide a definition of the information security culture (Chia et al., 2002). The current study findings do, however, add to knowledge about several information security culture features, that can help to articulate a sound definition. Each of these features appears to be unique to the information security culture concept; these features are:

- **Complex and difficult process:** The manifestations of information security culture do not exist independently, they are interrelated factors. In practice, the identification and examination of these mutual interactive relations calls for a complex and difficult process.

  As the current study data showed, the information security culture was seen as a product of socio-technical elements. These socio-technical elements involve elements of human behaviour, management activities and technological countermeasures that support the creation of information security culture.

- **Dynamic culture:** As the current study argues, information security by its definition is a continuous process. Given the dynamic and changing business environment, the original policies and procedures are subject to ongoing change. Implicit in this argument is the view that information security culture should be seen as a dynamic, flexible and ongoing process. This feature supports the idea that organisational culture in contemporary organisation is more of dynamic and flexible as opposed to the traditional view that culture is something which is bounded, fixed, and static over time. This is also supported by the emerging factor of change management (see Section 6.3.3).

- **Proactive and reactive culture:** Information security cultures can either a proactive or reactive or both. The data from the three cases indicated that Case A, was more proactive. For example, IT staff in Case A, were empowered to take all necessary actions to implement proven technologies and contingency plans were implemented, whereas, the approach in Case B and C leans to a reactive approach.

  It is crucially important to ensure that the IT department has easy access to proven technical solutions and necessary resources, which is why organisations are well advised to adopt a proactive approach. With the same emphasis, the current study further argues that organisations must adopt a reactive approach as well. This suggests that organisations should respond to changes and incidents related to information security efficiently and effectively. Information security culture, therefore, should be perceived as a proactive and reactive culture at the same time.

- **Short life cycle:** Information security culture cannot be sustained for an indefinite period of time. Once again implicit is the attribute of the dynamism, innovation brings new technology. The new technology usually brings new elements into the process by overriding most or all old elements (e.g. replacing access cards by a biometric system). The new system calls for a new security behaviour of the organisation's members. Therefore, what seemed to be effective information security practices before the introduction of the new technology cannot necessarily be effective any more.

> Besides the introduction of new technology, the findings of the current study revealed other events that support the short life cycle argument. One example is, when an organisation reconstruct its organisational structure, as in Case A, moving to concept of one platform. In the same fashion an organisation's expansion or downsizing appeared to support a short life cycle of specific information security practices.

Implicit in the proposed models and in the light of the four information security culture features discussed above, the current study articulates the following definition of information security culture:

Information security culture comprises all socio-technical activities and values that contribute to influencing individuals' intentions to perform practices that lead to the protection of all information properties (e.g. confidentiality, integrity, availability and accountability) in a given organisation in a given country.

The remainder of this section presents two models of information security culture that are based on a detailed analysis of the data collected from the three cases and from emerging themes and related literature.

6.6.1 Information security behaviour compliance model (Model I)

To understand the information security culture in an organisation, it is important to understand its information security environment, practices and issues.

While there are some normative models for information security behaviour which are reported to work for one or two firms, there is little in the way of general guidance. The research reported here thus represents an attempt to identify a descriptive measure of information security related behaviours that are applicable for different types of organisations.

Classification theory suggests that classifying perceptions is crucial to human survival and adaptation, and attempts to explain the nature of concepts (categories or classes) and why humans classify things (Smith and Medin, 1981; Parsons, 1996). Stanton et al. (2005) suggest that it is important to have a systematic view of end users security behaviour to facilitate accurate auditing and assessment of this behaviour. Therefore a classification that emphasises the characteristics of the organisations' staff who may perform authorised or unauthorised actions, is proposed as helpful to understanding individual information security behaviour. Such a classification may serve two purposes for an organisation. Firstly, categorising a phenomenon makes systematic studies possible, and secondly, classification may assist organisations prioritise their information security efforts.

The term "knowing-doing gap" refers to people who have knowledge but do not take action or behavior consistent with that knowledge (Pfeffer and Sutton, 2000). Workman et al. (2008) used this concept to investigate people's security behaviour referring to "people who have been trained but then do not use their new knowledge or skills as management expects". Following this analogy, the current study propose other possible patterns of an individual's behaviour with respect to information security practices. We choose to call these patterns modes (where mode means a "manner or way of acting, doing, or being; method or form") (Webster's New World Dictionary).

Based on an individual's acknowledgment of the security rules and the possession of the essential skills for performing certain actions, we identify four modes to categorise individual security behaviours: Knowing-Doing mode, Knowing-Not Doing mode, Not Knowing-Doing mode and Not Knowing-Not Doing mode. As mentioned in Section 5.1, data analysis was conducted to identify patterns and relationships between individuals' information security - related behaviours in the three cases. Figure 7.1 depicts these modes and their inter-relationships. Each mode is defined, theoretically justified from the relevant literature and supported with relevant example/s as follows.

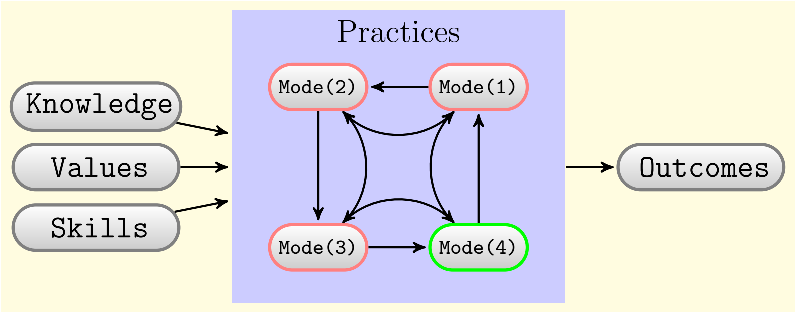


FIGURE 6.1: Information Security Behavior Modes

Mode(1): Not Knowing-Not Doing: In this mode, which falls into the upper right corner of the two-dimensional model of information security behavior modes, the subject does not know the organisation's requirements for information security behaviour and does not have security knowledge. As a result, they are not doing the right behaviour (violation of the security rules for behaviour - and security is compromised).

An example is a user who is not aware of the existence of organisational information security policies; he/she cannot be expected to follow them. Regardless of the presence of the necessary resources and the motivation to succeed, he/she can still fail to comply because they lack the knowledge of requirements or rules. An employee who has just joined the organisation or a manager who just been promoted to a new position may belong to this mode. This mode is a type of cognitive failure. Cognitive failures include issues such as: misunderstanding the security policy, missing an update of the policy, and poor decision-making.

In Cases B and C, individuals were not aware of their organisations' information security policies; hence, they could not be expected to act to follow them. As noted earlier, regardless of having the necessary resources and the motivation to do so, if an individual lacks knowledge of the requirements or rules he/she may not exhibit appropriate information security behaviour. This is a type of cognitive failure that also includes issues such as misunderstanding the security policy or missing an update of the policy. In Cases B and C there was no evidence to show that unified and / or clearly articulated information security policies had been communicated to users. The lack of understanding about policy appeared to be the main contributor to most of the non-compliance issues reported by Case B and C.

For instance, respondents from both Cases B and C raised the importance of organisational policies for the development of information security (e.g. policy that seeks to standardise managerial procedure). It also appeared that the lack of clarity about what kind of procedures needed to be followed and enforced contributed to the lack of information security compliance in Case C. Managers from different departments also supported IT staff views that the absence of clear information security procedures and directions had contributed considerably to information security system incidents. All the interviewees in Case C indicated that they were not familiar with the information security policy

Mode(2): Not Knowing-Doing: This second mode falls into the upper left corner of the model. The subject does not know the information security requirements and rules of behaviour and does not have security knowledge but is nevertheless doing the right security behaviour (following the rules - security is not compromised).

A subject who is not aware of organisation information security policies, but asks supervisors or co-workers before taking certain actions, is an example of this mode. Some people may exercise more caution than others when they are uncertain how to act. This prudent behaviour demonstrates the conventional economic concept of being risk averse. The concept of being risk averse suggests that, when facing choices with the same outcomes, subjects tend to choose the less-risky one (Friedman and Savage, 1948). To some extent, this mode is also traceable to the self-regulatory model, which identifies rule-following as ”originating within an individual’s intrinsic desire to follow organisational rules” (Tyler et al., 2007).

The data collected from the case interviews showed that most of the participants in the three cases were risk averse which, although they do not know predisposes them to act conservatively. This aversion was mainly attributed to the belief that taking risks could affect their organisation’s information assets. In Case A, and to a some extent, in Case B, a combination of self-consciousness as a member of the organisation and a willingness to abide by the organisation's rules indicated two aspects of both cases' organisational cultures. The first aspect was a sensitivity to losing information, knowing that they will be questioned about it. The other was the hope for a reward, through the KPI systems, as well as group bonus schemes, which were linked to organisational performance in Case A.

In a similar vein, all participants pointed out that cultural values can influence employees' information security related behaviours.

One can infer from the data that certain individual cultural values may have a positive or negative influence on employees' security behaviour. Most of the case data appears to support this claim, for instance respondents indicated that there is a cultural influence on individuals' security related behaviour which poses challenges, although managers may overcome these challenges by extended exposure to managerial activities such as training and/or awareness. However, some respondents did not see all personal cultural values as having a negative influence, especially in the context of individual security related behaviour.

This data indicates that some cultural values may impact on an individuals security related behaviour and ultimately influence information security culture in a positive way.

This last point can be further examined by understanding aspects of the relationship between managers and employees. As is common for national cultures that score highly on Hofstede's (1984) power distance value such as Saudi Arabia, executives and managers at upper-levels are sought out for advice and guidance (Hofstede, 1984). In a high power distance culture, employees usually rely on managers to solve work issues, because managers often attain the role of problem-solver. The influence of national cultural values (including power distance) was further discussed in the previous sections.

The data indicated that people may lack the experience to resolve problems since managers deal with issues in the absence of explicit procedures. Under these conditions, undesirable employee information security behaviour and actions may be minimised as most activities have to be approved by immediate managers or work supervisors.

Although negatively affected by the lack of sharing and motivation mechanisms, some employees have adopted informal means for sharing information and knowledge related to information security systems. Members of Case A, for example, meet after work and the conversation usually turns to something that happened during their work hours. Whenever the group are together they discuss issues and problems encountered in their daily work.

Mode(3): Knowing-Not Doing: In this third mode, which takes the lower left corner of the model, the subject knows the rules of behaviour and has the required knowledge and skills, but is not doing the right behavior (violation of the rules of behaviour - security is compromised).

Given their knowledge, skills and sometimes authority over others, it seems reasonable to expect that employees will comply with the requirements and rules. However, this is sometimes not the case. An example of this mode is a person who has been trained but then does not use his/her new knowledge or skills as management expects (Workman et al., 2008) or a top manager or IT staff member who takes advantage of his/her position to compromise the rules (Dhillon, 2001). This mode suggests that while knowledge and skills are a key contributor to users behavioural output they are not the only ones. Theories of cognitive psychology explain why people may behave irrationally. One explanation is that a person's set of beliefs, or culture, may influence their actions. This suggests that if a person has a tendency to perform an authorised act and this tendency needs to be influenced, one has to focus on changing their primary belief system (Dhillon, 2001). In this regard, Dhillon suggests that exposing employees to information about the consequences of their actions may produce a change in their behaviour.

The data revealed that there was careless risk taking where individuals may use shortcuts, downloading internet software and surfing harmful internet content. The extent of these practices, as noted, varied between the three cases. In Cases B and C individuals' behaviour can be attributed mostly to the lack of and poor clarity about the rules and consequences of taking information security risks. Whereas in Case A, the data indicated more intentional incidents related to non-compliant behaviour than a lack of rules and information about consequences. For example, Case A's intranet sites are updated regularly with security information, and employees are encouraged to access these sites on a regular basis. However, there was a perception that many of the organisation's members did not take these types of routine information security awareness programs seriously.

Mode(4): Knowing- Doing: In this mode, which takes the lower right corner of the model, the subject knows the rules of behaviour and has the knowledge and skills and they are doing the right behaviour (following the rules - security is not compromised).

This mode is based on the assumption that employees are rational actors who will comply with requirements because they have the necessary knowledge and skills. This mode is based on the view that people follow rules as a function of cost-benefit analyses (Stout and Blair, 2001). As in the case of Mode 2, Mode 4 is also linked to the self-regulatory model. While mode 4 appears to be the *"perfect mode"* for management to target, there are at least two reasons why it is risky to rely on this mode alone. The first reason is that the information system security discipline is rapidly evolving as is the threat environment, and the required level of knowledge and skills. Yet, Mode 4 assumes that actors are able to keep their knowledge and skills current. This has always been a major challenging and costly task. The second reason is that it is not enough to secure the system by relying on those subjects who have the knowledge and skills and are doing the right behaviours. Mode 4 requires the same level of planning, monitoring and managing as the previous modes. Furthermore an employee's behaviour may change from one mode to another, depending on their organisational role, the state of technology development and the status and availability of security training.

The level of information security culture of all three cases indicated that the majority of their members' information security related behaviour fitted in this mode.

Data showed that members of all three cases believed that the organisation's dependence on information systems is “very high and security is an integral part of this equation”. Most participants in all cases, indicated that there was a certain level of comfort with the progress that their IT department was making in information security related areas. For example, in each case, the data showed that the top management commitment to information security was exemplified by allocating the necessary resources and adopting technical solutions that were necessary to enhance their information security programs. The influence of national cultural traits (for example, Hofstede's power distance value) may be seen in the practices associated with this mode. Saudi Arabia is a high power distance society, and data from all three Cases indicated that individuals intended to follow the expectations of management and they are more likely to approve actions that they perceive to be supported by middle managers and work supervisors. These traits appear to be having a substantial influence on individuals' information security related behaviour in the three case studies.

Furthermore, the data indicated that a combination of self-consciousness as a member of the organisation and a willingness to abide by the organisation's rules was present in the three cases' organisational culture. The sensitivity of losing information, knowing that they will be questioned about it and the hope for a reward were also key factors in individuals' compliance with information security requirements.

However, as previously discussed, we should expect organisations' actors to keep their knowledge and skills current. It is not enough to secure the system by addressing the concern of those who have the knowledge and skills to do the right things alone. Organisations are going through a rapid and costly change as they seek to adjust and perform in the changing environment (e.g. new regulations, new technology and new threats). Therefore, Mode 4 requires the same level of planning, monitoring and managing as the previous modes. An employee's behaviour may alter from one mode to another, depending on the organisational role that the subject happens to be in, the state of technology deployment, and the prevalence and availability of suitable training.

The findings supported the proposed model of the four modes of information security behaviour. These findings were consistent with the view that an individual actor's decision to comply with security requirements is not only a function of their knowledge and skills or the perceived cost-benefit of the behaviour as described in economic theories, but also, a function of the factors arising from the users' psychology and the social setting in which the actor is situated. Therefore, it is crucial to understand how aspects of organisational and national culture inform employees' practices in order to achieve a high level of information security culture.

These findings provide a basis for us to propose further mode *"the information security culture mode"*. In this mode, organisations would work toward developing an information security culture where all employees adhere to its information security policy and rules even when no one is around and when their behaviour is not being monitored. Practices in Mode 5 would also include cooperative information security, such as taking action against acts that would jeopardise the information security system, for example, reporting unauthorised acts and sharing security related information and knowledge through the appropriate formal and informal channels.

We conclude this section with three remarks. First, although individual knowledge and skills are important, they alone are not enough to assure a positive contribution towards information security culture, which is partially reliant on employee behaviours. Second, a person's set of beliefs, or personal culture, plays a major role in influencing their personal attitude towards their security behaviour. Hence, understanding their underlying beliefs is crucial in the process of behavioural change. Third, the influence of technology, the social environment, regulation and self-interest all contribute to employees' security related behaviours. As a result members of an organisation could exhibit behaviours from different modes at different points in time. This continuous movement makes it hard to secure an organisation's information system by addressing a single mode in isolation.

Therefore, it is crucial to understand how aspects of organisational and national culture inform employees' practices in order to achieve a high level of information security culture. This argument is consistent with Schlienger and Teufel (2003) suggestion, in that an organisations information security culture should cover all the assumptions, beliefs and behaviours. However, there is no study that has empirically examined the influence of both the national and organisational culture on information security culture development. Thus, the current study is significant, both in terms of being the first to examine information security culture at both levels of their values, and in terms of reporting the relationships between the two dimensions.

To this end, an effort had been made in this study to examine the influence that organisational culture, national cultural values and technology may have on the information security culture development in the Saudi Arabia organisation context. Based on a synthesis of the study findings and emergent themes, a proposed holistic and relational model is presented in the forthcoming subsection.

6.6.2 Information security culture model (Model II)

The findings from the three cases studied show that some activities and behaviours in information security culture are more directly steered by technology, national and organisational cultures. This supports the idea that the cultural backgrounds of people in developing countries influence the effectiveness of certain activities, which is not the case in developed countries (Chen et al., 2006). This was evident from the public and non-profit cases, where the influence of some national cultural values was seen to play a major role in most of organisational and individuals' practices related to information security culture.

The information security culture in developing countries is, therefore, not limited to an organisation's setting. Rather, as the findings of the current study revealed, information security culture seemed to be influenced by internal elements from management activities, technology, organisational culture and external elements of national cultural values as well. More specifically, information security culture was seen as the result of applying a set of rules and procedures consistently along with technical countermeasures. The findings of the current study further suggest that some national cultural values can also stimulate and enrich conditions for information security culture creation. The positive values should be an emerging emphasis for organisations' management in creating information security culture.

An important consideration for an information security management framework is to address different approaches to information security culture, which can be systematised with a view of developing a holistic and relational framework. As discussed, information security culture can be viewed as consisting of several dimensions where organisational culture and national cultural values and technological factors influence organisational information security culture development.

In light of this discussion, the current study calls for a comprehensive analytical approach, in order to manage a complex phenomenon, to help develop understanding of the organisations' internal and external context for the creation and deployment of information security culture. As the findings suggest, the information security culture concept is not primarily one department's or one an individual's responsibility, but is more of a participative and collaborative process. Ensuring the protection of an organisation's information assets is no longer dependent on primarily hierarchically structured and controlled entities, but rather, is everyone's responsibility. Every member in the organisation has to participate actively in the process of protecting the organisation's information assets. Thus, emphasis should not be limited to individuals' status or position in hierarchies, but to everyone's willingness to abide by the rules, to enforce them, and to share information and knowledge relevant to the effectiveness and protection of the organisation's information systems. As the findings suggest, the failure to comply with information security policies appeared to be a failure of enforcement, not a lack of existence of those policies. In other words, in order to create an information security culture, organisations need truly to have mechanisms of enforcement in place. The enforcement mechanism can be comprised of both managerial and technical countermeasures in the first instance. If this vital process does not take place, then the security culture will not be there.

More specifically, organisations should work towards developing information security culture where all employees adhere to its information security policy and rules even when no one is around and when their behavior is not being monitored. Not only this but what is also needed is exercising cooperative security practices, by taking action against others' acts that would jeopardise the information system, for example, reporting unauthorised acts and sharing security knowledge and information through the right channel.

A central objective of the current study was to propose a unified, analytical and conceptual framework for understanding the roles of social, technical, and organisational factors, as well as the nature of their interdependencies, in the process of exploring information security culture. In the light of the above discussion, we can infer the way in which information security culture manifests itself within an organisation. Information security culture manifests itself in security related: values, behaviors, attitudes, actions, management related activities and physical environment.

The conceptual framework that was developed based on an extensive literature review at the start of the current study (see Figure 3.6), guided the development of questions for the interviews' protocol and the analysis process of the data. Evidence from the three case studies is used to substantiate or modify the relationships, and to identify new values or factors that appeared to influence individuals' information security related behaviour in organisations.

On the basis of the evidence provided by the three case studied, the conceptual framework was revised to present a model of an information security culture development and deployment, Figure 7.2 provides details of the model. The current study findings supported the identified groups of values and factors such as national culture, technical and organisational factors that may affect the the effectiveness of information security culture. The expected relationships between the four group of factors and information security culture have already been discussed and models have been proposed in the previous sections.

In determining what attributes to examine in relation to information security culture, the present study suggests a number of specific attributes that can be proposed:

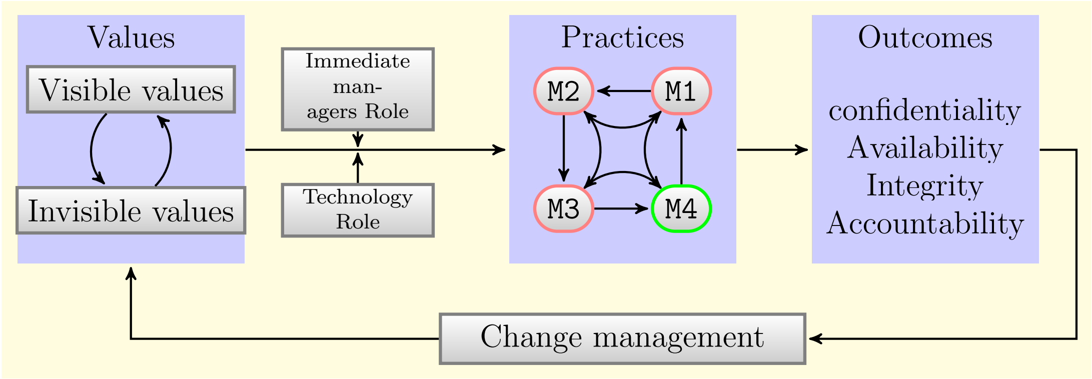


FIGURE 6.2: Information security culture model

The first two attributes can be viewed as corresponding to Schein's (2004) three levels model:

- **Visible activities:** These visible manifestations may include any activities which organisations can perform to either optimise their information security culture or adapt them to emphasise and achieve information security culture through appropriate management and employee behaviours. These may include any physical environment and management related activities (e.g. commitment of top management, security related standards, policies, procedures, training and awareness programs on information security related attitudes and behaviour for members of specific organisations).

- **Invisible values:** These capture the assumptions, attitudes, beliefs, values, and norms related to members of specific organisations in a given country. These are conceptualised by the organisational culture and national cultural values, which are believed to have influence on the information security related behaviours of an organisation's employees. The current study findings have clearly shown that information security practice is influenced by a set of both organisational and national cultural values.

- **Information security practices:** Information security practices relate to the actual security related behaviour of an organisation's employees that appears to be influenced by values and activities relevant to the technological, organisational and national cultural aspects. In this study, a model of individual behaviour was proposed and supported by the study findings (see Section 6.1, Figure 6.1). Thus, the Four Modes model was integrated in this model to present the possible information security practices in any organisation. For example, there may be compliance with the organisation's information security requirements or non-compliance. Security practices may also come in the form of adherence to security standards or regulations, such as the 7799 Standard.

- **Outcomes:** The outcomes that serve as a desired output to protect the information properties of confidentiality, integrity, availability and accountability.

- **Change management:** This represents the relevant initiatives to emphasise or change the status quo to achieve information security culture through appropriate management and employee behaviours. As threats increasingly evolve and technology changes then the context within which that organisation operates will become more vulnerable to various threats. The introduction of new technologies and business practices may lead to integrations and transformations between various aspects of information related values, assumptions and behavior. An organisation that fails to maintain an effective presence in these reconfigured arenas will find itself increasingly subject to severe threats from inside and outside.

- **Mediating factors:** These relate to factors through which the influence of values is mediated. The current study results suggest two factors accounted for most of the mediating influence between values and individuals' information security practices. Firstly, there is the role of immediate managers and supervisors. The development of information security culture is likely to depend on their ability and capability to enforce related rules and procedures and to facilitate the creation of a collaborative environment. The second factor relates to the role of technological countermeasures (e.g. information security mechanisms, such as access controls, digital signatures and firewalls) and the in-house vs. outsourcing aspect. The current study argues that without complete control over the information security technology, at least those related to the core business of an organisation, the information security culture is likely to be affected.

Figure 7.2 shows that the visible activities, invisible values and mediating factors will shape the intention of individuals related to information security culture. The arrows between the visible activities and invisible values indicate that each one of them can override the influence of the other. The model also illustrates the importance of change management as a tool to monitor and control changes that are associated with technology development and threats by applying the learning loop.

In summary, the model provides a systematic approach to develop and deploy organisational information security culture. The model is generally applicable to all contemporary organisations.The model links theories and findings from the case studies to facilitate information security management by providing a holistic analytic framework that can be used to develop and deploy an organisation's information security culture.

6.7 Summary

The research was conducted to answer three questions that related to an enrichment of the nexus between information security technology, organisational and national culture and information security culture development and deployment in three case studies in the Saudi Arabia context. In that regard, findings accompanied by explanations and implications (where relevant) were presented in this chapter.

The overall findings constituted an overall view of information security culture in the three case studies. The findings also indicated that there was a nexus between organisational and national culture and information security culture development and deployment in the three case studies in the Saudi Arabia context, the nature of which was further elaborated by the attendant explanation and interpretation.

Furthermore, a model was proposed encompassing all factors that appeared to influence the development and deployment of information security culture.

Chapter 7

CONCLUSION

7.1 Overview

Contemporary information security management recognises the imperative to include people and processes, as well as the more traditional technology security issues, in ensuring the quality of information in all modern organisations. To a large extent technological solutions for the majority of security issues have been previously developed. There are however still many application challenges involving the people and processes components of information security management. This leads to the need for a socio-technical approach in focusing on these issues in technologically developing countries.

Thus, the human factors represent a key issue that has to be addressed by managers for effective information security management to take place. It is necessary to identify those human elements, which affect the whole system's effectiveness in order to design strategies that can minimise their weakness. Therefore, when analysing information security systems, it is necessary to look at organisations' information security systems in a socio-technical context.

The current study is significant; both in terms of being the first, as far as the researcher is aware, to examine information security culture at the levels of both organisational culture and national cultural values, and in terms of reporting the relationships between these two and information security culture. Explicit benefits of this contribution include highlighting values and factors that appeared to be unique to the context of developing countries, specifically to organisations in the Saudi Arabia context.

This study clearly shows that individual's security related behaviour is one of the most critical and complex issues to be managed. There is a need for knowledgeable management that understands the importance of managing information security and providing information security managers with enough support and authority to improve information security development. The current study offers empirical evidence of a set of interrelationships between important values and factors that tend to pertain to the development and deployment of information security culture within the context of a country with rapidly technologised systems, Saudi Arabia.

The remainder of this chapter concludes the thesis and discusses the study's outcomes in light of their contributions, significance and limitations. Firstly, there is a presentation of how the research questions have been addressed. Then, some conclusions are drawn in regards to implications of the study for research and information security development practices. Finally, the chapter presents the research limitations and suggestions for future research.

7.2 Questions addressed in this study

This research set out to address the following problem:

What organisational elements need to be addressed or managed to ensure effective information security management in the Saudi Arabia context?

The motivation for this research was to resolve this problem and thereby provide a body of useful recommendations for organisations' managers and implementers of e-government programs in the Saudi Arabia context.

In order to resolve this problem, three research questions were formed, which were as follows:

1) What are the current management practices in relation to information security management and influencing cultural factors in the context of Saudi Arabia?

In order to conceptualise the cultural values and factors influential to information security management overall, a synthesised literature review from various perspectives capturing information security management's factors and values was conducted. The current literature on information security management, social-technical aspects, information security culture as such and the case of Saudi Arabia were reviewed.

Based on the literature from these various perspectives, a conceptual framework was proposed for a detailed investigation involving a case study approach to determining the feasibility of the existence of national and organisational factors influencing information security culture within three cases in the context of Saudi Arabia.

2) To what extent do the dimensions of both organisational and national culture influence individuals' related information security practices?

Studies have argued that national culture has more influence on members of an organisation than organisational culture (e.g. Oliver, 1997) , while others have argued that organisational cultures are more influential than national cultures (e.g. Nelson, 2003; Pothukuchi et al., 2002; Selmer, 1996). In order to establish a deep focus for this research study, a particular aspect of information security management, the dimensions of both organisational and national culture, were more thoroughly investigated.

Through this question, the influence of organisational and national culture on the information security culture and the impact they might have on development and deployment of the information security culture were investigated. More specifically, this question was addressed by considering the following two sub-questions:

S-RQ1: To what extent do the relevant values of national culture that influence the effectiveness of information security management?

In response to this sub-question, the national culture values of (Hofstede 2001 and the context value of Hall1 976) were included in the conceptual framework, thus enabling the capture of national culture values' influence on information security culture development and deployment. More specifically, the national culture dimension was conceptualised by the four national cultural values of Hofstede's (2001) (power distance, uncertainty avoidance, individualism vs. collectivism) and Hall's (1976) values of context, which are believed to have influence on the information security-related behaviours of an organisation's employees.

As mentioned in previous chapters, national culture is fairly difficult to quantitatively capture. Hence, it was necessary to investigate culture through qualitative interviews. As part of the data collection process described in the previous chapters, participants were asked open ended questions about cultural values and their role in information security culture development.

Overall, the analysis of the three cases revealed that national cultural values significantly influence the broad adopted towards information security management. These values did act to shape, in a negative or positive way, the processes and decisions related to information security management. However, while the national cultural values appeared to have a fundamental influence on the three cases, variations of the degree of influence were found in each. These variations can mainly be attributed to differences in the organisational efforts to promote information security management in each case and to the sectors that each case is operating in (government, public or non profit). Section 6.2 provided more discussion on the national cultural influence.

S-RQ2: To what extent do the relevant values of organisational culture that influence the effectiveness of information security management?

In response to this question, the current study included the organisational culture dimension in the research framework. The influence of organisational culture was also addressed through the case study. Information was obtained on the operational activities that support the existence and/or attainment of some form of information security culture performed by organisations and their members in each of the case studies. These comprise top management commitment, the training program, the awareness program, the IT structure, the appointment of information security managers, the type of motivation system utilised, the existence of information security policy and adoption of information security standards. The key disclosure was that the influence of organisational values and management activities on the information security culture within the three cases appears to be relatively uniform. Section 6.1 presented the findings on organisational culture.

As these sub-questions were answered and explored in the course of the research, a model emerged which classifies and organises the characteristics of organisational subjects involved in the information security practices. This framework expands on the traditional human behaviour and the social environment used in social work by identifying how knowledge, skills and individual preferences work to influence individual and group practices with respect to information security management (refer to Figure 7.1).

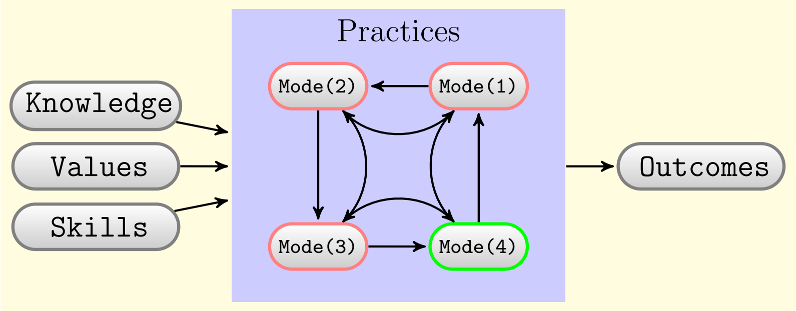


FIGURE 7.1: Information Security behaviour Modes

The findings revealed the existence of the four modes of information security behaviour in the three cases studied; a number of factors appeared to be interrelated. These inter-related factors were organisational culture values manifest in practices and activities related to information security management and values related to the national culture. Hence, these findings are consistent with the view that an individual actor's decision to comply with security requirements is not only a function of the his/her knowledge and skills or the perceived cost-benefit of the behaviour, as described in economic theories, but also, a function of the factors from the users' psychology and the social setting in which the actor is situated. Therefore, it is crucial to understand how aspects of organisational and national culture inform employees' practices in order to achieve a high level of information security culture. The results also suggest how these values are related to the individuals intention to engage in information security related behaviours.

3) How can organisations achieve a quality and successful information security culture with respect to the proposed framework that satisfies requirements of the Saudi Arabia context?

The results of the exploratory studies as well as the empirical study provided unanimous agreement for supporting the information security individuals behaviour model introduced by this research. Both frameworks, the information security individuals' behaviour model and the cultural framework were incorporated in one main framework to present a holistic model that could be utilised to develop and deploy an information security culture (refer to Figure 7.2).

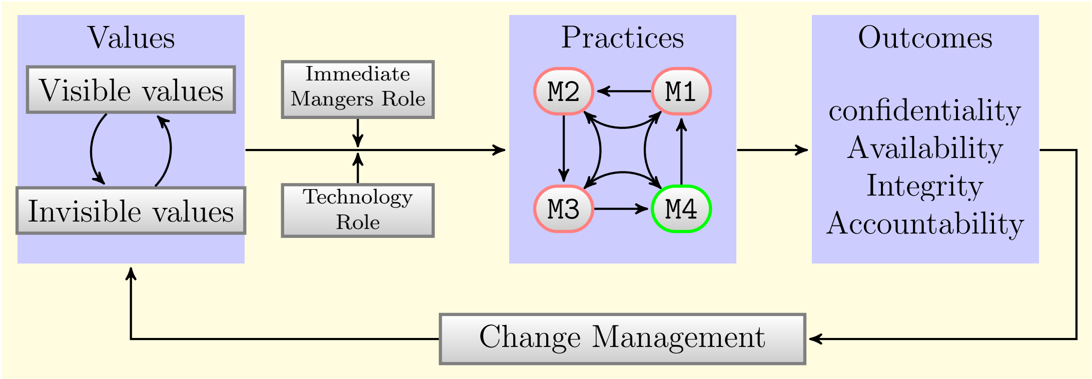


Figure 7.2: Information security culture model

Hence, the introduced model is a step towards developing a theory of cultural effect on individuals information security behaviour. This research has drawn a variety of theories from diverse disciplines such as cultural studies, Human behaviour, and information system management. An in depth study of three cases was used for data collection and analysis. Therefore, it is argued that data, theory and multidisciplinary triangulation were achieved consistently throughout the different phases of the research.

For organisations in the Saudi Arabia context or organisations with similar constraints, the model could be used to develop and deploy an information security culture in their settings .

7.3 Contributions

The current study presented a comprehensive analytical conceptual framework by combining prominent theoretical perspectives in one model of information security culture as follows.

First, the current study presented a comprehensive analytical conceptual framework of individuals' information security compliance behaviours. The proposed framework provides descriptive measures that are applicable for more than just specific organisations.

Second, this study contributes new insights into the influence of the national culture values. Hence, the national culture values were adopted for the information security management domain, providing a lense that may also be used in other related studies in similar contexts to develop greater and deeper understanding.

Third, the influence of organisational culture values on the development and deployment of information security culture was addressed by incorporating the organisational values and factors that were believed to have an influence on managers' and employees' information security behaviour. The relationship between these important dimensions is not thoroughly researched. The information security culture model (Figure 6.1) showing important facets of technology, national and organisational culture's influence on information security culture enactment offers a new contribution to the field and may provide opportunities for future research and development.

Furthermore, the findings of the current study contribute new insights into the concept of information security culture, which is a concept that does not have a clear definition Chia et al. (2002). Based on the findings of this study, a definition of information security culture and four relevant attributes were proposed that could help in our understanding of this complex concept. Each of these attributes appears to be unique to the information security culture concept. The attributes are: **complex and difficult process**, **dynamic**, **proactive and reactive** and a **short life cycle** culture. The aspect of each attributes and interrelationships have already been discussed and proposed in the previous chapter (Section 6.6).

7.4 Implications

The conclusions from the current study have a number of implications for academia and organisational practice and these are as follows:

Theoretical implications:

- In terms of theory building, this research integrates and extends well-accepted models and then applies the proposed model in a cultural context. This research explicates the role of organisational culture values in establishing information security culture, integrates these factors with the individuals' behaviour modes framework and then shows how the integrated model is affected by four national cultural values. The outcomes then present the effectiveness of information security in terms of the information security principles (confidentiality, integrity, availability and accountability). Further, to address the attribute of dynamism within information security culture, the present study, proposed the approach of change management to manage such issues related to this attribute. The information security culture model proposed by this research is illustrated in Figure 7.1.

- From a theoretical perspective, the study endeavours to break new ground by analysing private, public and non-profit organisations through an organisational and national culture lens in an information security setting. It contributes to the existing body of theory on behaviour, organisational and national culture theories by applying those theories to three types of organisations in a developing country, specifically in the Saudi Arabia context, thus attempting to bridge a gap that exists in the domain of information security management.

- It also contributes to the public vs. private management literature by shedding light on the human processes that appeared to facilitate the development and deployment of information security culture. The study contributes to information security management by providing a behaviour compliance model in an information security setting. It adds to organisational theory by building on the ongoing discourse of how organisational forms affect performance.

- From the perspective of research methodology, the current study further contributes to the advancement of the interpretive tradition in information security management system research. Although the interpretive paradigm has long been established in the information system literature (Walsham 2006), applying this paradigm to an information security setting may help to advance the field. The methodology is linked to the theory in that it illustrates how to apply the research framework and analysis required to examine the influence of several of socio-technical aspects on the development of an information security culture.

  This study also demonstrates that qualitative methods, specifically the case study method, were found to be valuable to explore new insights as well as to develop potential relationships between constructs.

- The present study contributes to the research on information security management in three important aspects:

  - Firstly, this may be the first study that empirically investigates the influence of national culture in an information security context.
  - Secondly, this study developed a model to define the construct of information security culture. This framework provided a view of understanding the determinants of the national and organisational culture values and security mechanisms that were seen to directly affect the development and deployment of information security culture.
  - Thirdly, this study presents a model for classifying and organizing the characteristics of organisational subjects involved in these information security practices. The model expands on the traditional perspectives of human behaviour and the social environment used in social work by identifying how knowledge, skills and individual preferences work to influence individual and group practices with respect to information security management. The classification of concepts and characteristics in the framework arises from a review of recent literature and is underpinned by theoretical models that explain these concepts and characteristics.

- The present study contributes to the research of cross-culture by stressing the role of human and management aspects (national and organisational culture values) as main contributors to individual's information security behaviour. This study provided empirical evidence that supports the study's hypotheses, in that national and organisational culture values appeared to influence individuals' intentions and practices related to information security behaviour in the context of developing countries.

  The adoption of three of Hofstede's national culture values (power distance, uncertainty avoidance, and collectivism) and Hall's high context value aimed to check whether the national cultural values of Saudi Arabia influence individuals' practices relevant to information security.

  - In regard to the value of power distance, the case data seemed to suggest that there was no influence of this value on individuals' practices related to information security at the upper level of the organisational hierarchy. However, the data appeared to suggest such influence is likely to be found at the low level of the organisational hierarchy in all three cases. In the contrast, the influence of the uncertainty avoidance is likely to be found only at the upper level of the organisational hierarchy in all three cases.

  - With respect to the value of collectivism, the case findings seemed to suggest that there was strong influence of this value on individuals' practices related to information security at the upper and low level of the organisational hierarchy in the three cases, to a different degree.
  - The present study findings also support the view that Saudi Arabia culture as an Arab country is neither collectivist as in Asian societies nor individualist as in western cultures (Elashmawi, 1993).
  - In regard to Hall's value of high context, the present study indicates that high context appeared to play a crucial role in participants' communications that were relevant to information security in the three cases.

  Thus, the research contributes to the body of cross-cultural research by providing a deeper view of Hofstede's cultural model for the Saudi Arabia's culture. However, as suggested earlier, caution should be taken in generalising this conclusion as the domain of information security management, by its nature, is associated with close supervision and direction as well as restricted rules and procedures that must be followed.

- Furthermore, for academics, it has provided a case-study illustration of information security culture, from which future research can take reference and build upon.

Practical implications:

The present study offers several important managerial implications. The practical contribution rests in the ability of organisations' information security managers to be able to develop and deploy an information security culture. By better understanding the power relationships that impact the complex nature of regulating a social system, information security managers may be best able to create and deploy an information security culture for their respective organisations. The emergent findings revealed several specific areas that practitioners could find of use in establishing such a culture. These practical implications can be used as a guideline by organisational information security managers to assist in developing and deploying an information security culture. A highlight of the key practical implications related to the development of organisation's information security culture are presented below:

- Improvement in organisation information security culture is imperative in the success of information security management. Therefore, equal attention should be given to both information security technology and management aspects.
- This study proposed that national and organisational as well as security mechanism are an important determinant of organisations' information security culture in the context of developing countries.
- The research highlights the importance of organisational values and factors such as top management commitment, the level of training and IT skills, security awareness programs, organisational IT structures, the appointment of Information Security Managers, the type of motivation system utilised, the existence of information security policy, and adoption of information security standards as determinants of information security culture creation.
- Other factors were related to the influence of national culture on values in decision making, compliance, risk taking, sharing, collaboration, enforcement, reporting, and communication.

- Furthermore, technical factors were reported to play a role in the development of information security culture in Saudi Arabia organisations, such as, difficulties and limited use of information security management standards and the shortage of trained IT staff particularly those who adequately understand and can implement information security standards.

- Although some large organisations are required to apply standards and are considered as pioneers in Saudi Arabia, public and non-profit organisations have not embarked on standardisation. It is the current study's view that in order to achieve efficiency and effectiveness of information security culture, all organisations in Saudi Arabia should move towards the adaption of information security management standards.

- The current study argues that while the decision to outsource was justified by the related workforce deficiency, there were some concerns about the negative influence of this factor on the enhancement of information security culture in terms of both information confidentiality and availability principles in the long-term.

- The current study also suggests that certain management practices such as the creation of a partnership with Human Resources to better identify training needs, employee sensibility, recruitment and selection and wages being linked to management by competencies and focusing on information security issues all appeared to have direct influence on the enhancement and sustainability of organisation information security culture.

- The study also found that technical countermeasures can play a major role in shaping individuals' security related behaviour by adjusting those of negative values and encouraging positive ones. The research also provides empirical evidence on the significant role of the immediate managers in establishing an effective information security culture.

- As the findings suggest, the concept of information security culture is not primarily one department's or one individual's responsibility, but is more of a participative and collaborative process. Ensuring the protection of an organisation's information assets is no longer dependent on primarily hierarchically structured and controlled institutions but rather is everyone's responsibility. Every member in the organisation has to participate actively in the process of protecting that organisation's information assets. Thus, emphasis should not be limited to individuals' status or position in hierarchies, but to everyone's willingness to abide by the rules, to enforce them, and to share information and knowledge relevant to the effectiveness and protection of the organisation's information security systems.

- This also suggests that the failure to comply with information security policies appeared to be a failure of enforcement, not a lack of existence of those policies. In other words, in order to create an effective information security culture, organisations need truly to have mechanisms of enforcement in place. The enforcement mechanism can be comprised of both managerial and technical countermeasures as a first principle. If this vital process does not take place, then the security culture will not exist.

- Furthermore, one aspect that seems to be essential for a quality information security culture is to consider the natural trade-off created by two major concepts: scope and risk. The trade-off occurs because in general organisations ask employees to accomplish more things (scope) with less (risk). How management of the organisation solves the trade-off formed by these seems to be a determinant of their success in achieving a quality information security culture.

- The researcher believes that the population and information security systems in all organisations are sufficiently similar to many other organisations in Saudi Arabia, so it is not unexpected that the results, outcomes and conclusions may apply to the other organisations and other countries with similar constraints. As the Arab countries share many cultural characteristics (Hofstede, 2001), it is also believed that this picture can be used to describe the behaviour towards development and deployment of information security culture for other Arab organisations. Particularly, the present studys findings are believed to be applicable to other developing and Arab countries that share basic national and demographic characteristics with Saudi Arabia such as the GCC countries.

7.5 Limitations

The scope of this study is limited to organisations in Saudi Arabia. The respondents are mostly key IT management employees, such as IT security officers and function managers.

Theoretical limitations:

The present study relies primarily on the extensive work of Hofstede (2001), Hall (1976) and Chia et al. (2002). The current study relied on those frameworks because they cover both the organisational culture values and the national cultural values.

These are limited to those values and beliefs that are expected to have an influence on the information security management effectiveness, specific to the culture or ethnic group being studied. The focus of the current study was on understanding the organisations' perspective about the following: information security management, information and knowledge sharing and change management factors and issues. Some of the factors may overlap with each other, even though they originate in different fields. Other constructs such as economic, political and external regulations may be found to be as important, and the relationships between the various constructs may change. The possible influence of such dimensions may also be researched as they were not examined in this study.

Methodological limitations:

It is very difficult to generalise from case studies, especially single case designs (Darke et al, 1998). The implications for this are that the reliability and validity of generalisations to other organisations are very limited.

The findings of the three case studies could be applied to large Saudi Arabia or Arab organisations with a similar structure and capability. Having multiple case studies from different industries has greatly increased the ability to generalise, and perform cross-case analysis (Darke et al, 1998) of different approaches. Besides this, very rich data from multiple perspectives in the organisation, triangulated with documentation provided accurate findings. However, the generalisation of the results of this study should be treated with caution beyond the scope of this sample. Future empirical work is needed to demonstrate that these findings are not unique to this particular sample.

Although extensive precautions were taken to keep the organisations names strictly confidential, many organisations did not participate. The relatively small number of participants is of concern and as with all qualitative methods, the quality of the interview data depended entirely on the subjects giving truthful and comprehensive answers. Subjects might have misrepresented their meanings. The protocol of question design helps to lessen this concern. The questions were grouped in two sections (see Appendix A). The two sets were designed to be complementary to each other and to provide a cross-check on the discoveries. It has been designed in this manner to minimise potential bias through the application of common instruments, including the interview guide and supporting organisation documents.

Furthermore, the presence of the researcher in conducting face-to-face interviews with the participants also helped to filter out the less reliable data. However, qualitative research like this is always open to possible researcher bias and this is no exception. In this study, an attempt to counter this possibility was made by having participants review and comment on their answers and quoting the subjects' exact words as much as possible to let readers judge for themselves.

Finally, although case data was collected from multiple sources, (key IT management employees, such as Information Security Officers and IT managers, function managers and organisations' policies,reports and websites), the case studies would have been strengthened by interviewing more low level users to elicit their perspectives about the information security issues.

7.6 Future research

Several directions for the future stemmed from the emergent findings that were identified during the analysis of the data collected during this study.

It would be useful to test the overall research model in a quantitative study, expanding the sample to a representative size.

Furthermore, significant insights should be gained by extending the framework analysis of behaviour compliance to various types of domain, and by quantifying the strength of ties. Added value would also derive from measuring the modes dynamics over time.

Another possibility for future research involves examining how management of the organisation might mitigate the trade-off formed by scope and risk in the process of an information security culture development.

The results reached in this study are believed to assist Saudi Arabia's organisations and other countries with similar characteristics across key variables in the domain of information security management. Hence, comparative studies could be performed to match the findings of this study with other developing countries. By conducting a similar study on different countries that perhaps share basic characteristics with Saudi Arabia, the findings reached might be compared to the results of this study and affirm or extend its results. Also, by conducting a similar study on developed countries, the findings reached might be compared to the results of this study and affirm or extend its results.

It is very important to recognise, however, that if a global organisation is to be effective in managing its information system, understanding cultural differences is essential. Furthermore, a worldwide subculture of management is emerging, and one needs to know how to function effectively in it. For this reason, further research should be devoted to this area, and the limitation of the present study such as the small number of subjects and the overlapping of variables, should be taken into account.

7.7 Summary

This chapter concluded the thesis and discussed the study's outcomes in light of their contributions, significance and limitations. Firstly, there was a presentation of how the research questions have been addressed. Then, some conclusions were presented in regards to implications of the study for research and information security culture development and deployment. Finally, the chapter presented the research limitations and suggestions for future research.

7.8 Summary of thesis

The motivation for this research stems from the continuing concern of ineffective information security in organisations, leading to potentially significant monetary losses. Both dimensions of national and organisational culture has been identified as an underlying determinant of individuals' behaviour and this extends to information security culture, particularly in developing countries. This research investigates information security culture in the Saudi Arabia context.

Chapter 1 has introduced the need for a greater understanding of organisational elements associated with effective information security culture in the context of Saudi Arabia. The research questions, study design and potential contributions from the study have been presented. A background to the overall context of the study and the motivations and rationale for the study has also been provided.

Chapter 2 presented the literature analysis. It outlined the foundations of the study. The three main subject areas were reviewed: information security management, information security culture and the cultural dimensions of the Saudi Arabia context.

Chapter 3 presented the initial framework for the research derived from the literature, the dimensions of the framework and how they are derived were brought forth. This chapter concluded by presenting the analytical framework used in the research.

Chapter 4 presented the research methodology. A case study method was used. The chapter began with a theoretical perspective of the research methodology. The background for the selection of the case study method was discussed. Then, the case study protocol including data collection procedures was outlined including their relevance to each phase of the research and how they relate to the research questions. Finally, the data analysis strategy and processes were discussed, followed by a discussion of the issues associated with validity and reliability.

Chapter 5 presented and discussed the research findings that pertain to information security culture effectiveness for each of the three case studies.

Chapter 6 synthesised the findings from the three cases, and refined the conceptual model proposed earlier in Chapter 3.

Chapter 7 concluded the thesis by discussing the outcomes in terms of the research questions and in light of their contributions, significance and limitations. Recommendations for further research were outlined in this chapter. This concludes the thesis.

Bibliography

Abbas, A. (1993). Decision-Making Style, Individualism and Attitudes toward Risk of Arab Executives. *International Studies of Management & Organization*, 23(3):53–74.

Abu-Musa, A. (2007). Evaluating the security controls of CAIS in developing countries: An examination of current research. *Information Management & Computer Security*, 15(1):46–63.

Ajzen, I. (1985). *From Intentions to Actions: A Theory of Planned Behavior,*. Springer, Heidelberg, Germany.

Al-Gahtania, S., Hubonab, G., and Wangb, J. (2007). Information technology (IT) in Saudi Arabia: Culture and the acceptance and use of IT. *Information & Management*, 44(8):681–691.

Al-Jafary, A., AbdulAziz, and Hollingsworth (1989). Leadership styles, machiavellianism, and needs of Saudi Arabian managers. *Value Based Management*, 2(1):103–111.

Al-Yahya, K. (2008). Power-Influence in Decision Making, Competence Utilization, and Organizational Culture in Public Organizations: The Arab World in Comparative Perspective. *Journal of Public Administration Research and Theory*, 19:385–407.

Aljifri, A., Pons, A., and Collins, D. (2003). Global e-commerce: a framework for understanding and overcoming the trust barrier. *information Management & Computer Security*, 11(3):130–138.

Bakari, K., Tarimo, N., Yngstrom, L., and Magnisson, C. (2005). State of ICT Security Management in the Institutions of Higher Learning in Developing Countries: Tanzania Case Study. In *Computers & Security Proceedings of the Fifth IEEE International Conference on Advanced Learning Technologies (ICALT 05).*

Ball, A. and McCulloh, H. (1990). *International Business (4th ed.).* Homewood, IL: Irwin.

Bates, G. and Plog, F. (1976). *Cultural Anthropology.* 3rd Ed., New York: McGraw-Hill.

Benbasat, I., Goldstein, D., and Mead, M. (1987). The case research strategy in studies of information systems. *MIS Quarterly*, 11(3):369–386.

Berg, B. (1989). *Qualitative Research Methods for the Social Sciences.* Allyn and Bacon, Massachusetts.

Bjerke, B. and Al-Meer, A. (1993). Culture's Consequences: Management in Saudi Arabia. *Leadership and Organization Development Journal*, 14(2):3035.

Boudreau, C., Ariyachandra, T., Gefe, D., and Straub, D. (2004). Validating IS Positivist Instrumentation: 1997-2001. *published in the handbook of information systems research, M.E.Whitman and A.B. Woszczynski (eds). Idea Group Publishing, Hershey, PA USA, 15-26.*

Bouthillier, F. and Shearer, K. (2002). Understanding knowledge management and information management: the need for an empirical perspective. *Information Research, [Available at http://InformationR.net/ir/8-1/paper141.html]*, 8(1).

Bozeman, B. (1987). *All Organizations are Public.* San Francisco, CA: Jossey Bass.

Bozeman, B. and Bretschneider, S. (1986). Public management information systems: Theory and prescription. *Public Administration Review*, 46:475–487.

Bretschneider, S. (1990). Management information systems in public and private organizations: An empirical test. *Public Administration Review*, 50(5):536.

Campbell, D. (1975). Degrees of freedom and the case study. *Comparative Political Studies*, 8:178–185.

Caudle, S. L., Gorr, W. L., and Newcomer, K. E. (1991). Key information systems management issues for the public sector. *MIS Quarterly*, 15 (2):171–188.

Chang, E. and Lin, S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems*, 107(3):438–458.

Chang, S. E. and Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, 106(3):345–361.

Chapman, M. (1997). Preface: Social anthropology, business studies, and cultural issues. *International Studies in Management & Organization*, 26(4):3–29.

Chaula, A., Yngstrm, L., and Kowalski, S. (2006). Technology as a tool for fighting poverty: How culture in the developing world affect the security of information systems. In *Proceedings of the 4th IEEE International Workshop on Technology for Education in Developing Countries (TEDC06)*. IEEE.

Chen, Y., Chen, H., Huang, W., and Ching, R. (2006). E-government strategies in developed and developing countries: An implementation framework and case study. *Journal of Global Information Management*, 14(1):23–46.

Chia, A., Ruighaver, B., and Maynard, B. (2002). Understanding Organizational Security Culture. *Proceeding of PACIS2002, Japan.*

Choudhury, M. and Al-Sakran, S. (2001). Culture, Finance and Markets in Saudi Arabia. *Managerial Finance*, 27:25–46.

Ciganek, A., Jarupathirun, S., and Hangjung, Z. (2004). The Role of National Culture and Gender on Information Elements in e-Commerce: A Pilot Study on Trust.

CITC (2006). Communication and information technology commission annual report (2006). Technical report, CITC.

Clugston, M., Howell, J., and Dorfman, P. (2000). Does cultural socialization predict multiple bases and foci of commitment? *Journal of Management*, 26(1):5–30.

Conklin, W. (2007). Barriers to adoption of e-government. In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on system sciences. IEEE.*

Crotty, M. (1998). *The Foundations of Social Research: Meaning and perspective in the research process.* London, Sage Publications.

Currie, L. (1996). Organizational structure and the use of information technology: Preliminary findings of a survey in the private and public sector. *International Journal of Information Management*, 16(1):51–64.

Denzin, N. and Lincoln, Y. (2003). *Strategies of Qualitative Inquiry.* Sage Publications, Second edition.

Detert, J., Schroeder, R., and Mauriel, J. (2000). A framework for linking culture and improvement initiatives in organisations. *The Academy of Management Review*, 25(4):850–863.

Dhillon, G. (1995). *Interpreting the Management of Information Systems Security.* London: London School of Economics and Political Science.

Dhillon, G. (1999). Managing and controlling computer misuse. *Information Management & Computer Security*, 7(4):171–175.

Dhillon, G. (2001). Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns. *Computers & Security*, 20:165–172.

Dhillon, G. and Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, 11(2):127–153.

Dhillon, G., Tejay, G., and Hong, W. (2007). Identifying governance dimensions to evaluate information systems security in organizations. *Proceedings of the*

40th Annual Hawaii International Conference on System Sciences (HICSS'07), comuter security,IEEE.

Dhillon, G. and Torkzadeh (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*, 16:293–314.

Dibbern, J., Goles, T., Hirschheim, R., and Jayatilaka, B. (2004). Information systems outsourcing: A survey and analysis of the literature. *The DATA BASE for Advances in Information Systems*, 35(4):6–102.

Drucker, P. (1988). The coming of the new organization. *Harvard Business Review*, 66(1):4553.

Ebrahim, Z. and Irani, Z. (2005). E-government adoption: architecture and barriers. *Business Process Management Journal*, 11(5):589–611.

Eisenhardt, K. M. (1989). Building Theories From Case Study Research. *The Academy of Management Review*, 14(4):532–550.

Elashmawi, F. (1993). *Multicultural Management 2000: Essential Cultural Insights for Global Business Success*. Gulf Publishing Company, Houston, TX.

Eloff, J. and Eloff, M. (2003). Information Security Management A New Paradigm. In *Proceedings of SAICSIT 2003,130-136*.

Emory, C. and Cooper, D. (1991). *Business Research Methods*. Richard Irwin Inc., Boston, 4th edition.

Fishbein, M. and Ajzen, I. (1975). *Belief, attitude, intention and behavior: an introduction to theory and research*. Addison-Wesley, Reading, MA.

Friedman, M. and Savage, L. (1948). The Utility Analysis of Choices involving Risk. *Journal of Political Economy*, 56:279–304.

Fryer, J., Antony, J., and Douglas, A. (2007). Critical success factors of continuous improvement in the public sector: A literature review and some key findings. *TQM Magazine*, 19 (5):497–517.

Gerhart, B. (2008). How Much Does National Culture Constrain Organizational Culture? *Management and Organization Review*, pages 1740–8776.

Goldkuhl, G. and Lyytinen, K. (1982). A language action view of information systems. In *Proceedings of the 3rd International Conference on information Systems*, pages 13–30. The Institute of Management Sciences.

Grover, V., Jeong, R., Kettinger, J., and Teng, C. (1995). The implementation of business process reengineering. *Journal of Management Information Systems*, 12(1):109–144.

Hall, E. T. (1976). *Beyond Culture.* Anchor.

Hasan, H. and Ditsa, G. (1999). The impact of culture on the adoption of it: an interpretive study. *Journal of Global Information Management*, 7(1):5–15.

Hazlett, S. and Hill, F. (2003). E-government: the realities of using it to transform the public sector. *Managing Service Quality*, 13 (6):445–452.

Heeks, R. (1999). Centralised vs. Decentralised Management of Public Information Systems: A Core-Periphery Solution. *iGovernment Working Paper Series.*

Heeks, R. (2002). Information Systems and Developing Countries:Failure, Success and Local Improvisations. *The Information Society*, 18(2):101–112.

Heeks, R. (2003). Most egovernment-for-development Projects Fail: How can risks be reduced? *iGovernment Working Paper Series*, Paper no. 14.

Hilangwa, M. and Pervan, G. (2005). Designing a case study protocol for application in IS research. *In Proceedings of the Ninth Pacific Asia Conference on Information Systems.*

Hinnant, C. and Welch, E. (2003). Managerial capacity and digital government in the states: examining the link between self-efficacy and perceived impacts of it in public organizations. In *System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on Seystem Sciences.IEEE.*

Ho, A.-K. (2002). Reinventing local governments and the e-government initiative. *Public Administration Review*, 62(4):434–444.

Hofstede, G. (1980). *Culture's consequences: International differences in work related values.* Thousand Oaks, CA: Sage Publications, Inc.

Hofstede, G. (1984). *Culture's consequences: International differences in work-related values.* Beverly Hills, CA: Sage Publications.

Hofstede, G. (1991). *Cultures and organizations: Software of the mind.* London: McGraw-Hill.

Hofstede, G. (1993). Cultural constraints in management theories. *The Academy of Management Executive*, 7(1):81–94.

Hofstede, G. (2001). *Culture's Consequences, Comparing Values, Behaviors, Institutions, and Organizations Across Nations.* Thousand Oaks CA: Sage Publications, Second edition.

Hofstede, G. (2002). Dimensions do not exist: A reply to Brendan Mcsweeney. *Human relations*, 55(11):1355–1361.

Hofstede, G., Neuijen, B., Ohavy, D. D., and Sanders, G. (1990). Measuring Organisational Cultures: A Qualitative and Quantitative Study across Twenty Cases. *Administrative Science Quarterly*, 35:286–316.

Hone, K. and Eloff, P. (2002). Information security policy – what do international information security standards say? *Computers & Security*, 21(5):402–409.

House, R., Hanges, P., Javidan, M., Dorfman, P., and Gupta, V. (2004). *Culture leadership and organizations: The GLOBE study of 62 societies.* Sage, London.

Hunt, D. and Attwaijri (1996). Values and the Saudi Manager: An empirical investigation. *Journal of Management Development*, 15:4854.

Hutton, G. (1996). BPR-overcoming impediments to change in the public sector. *New Technology Work and Employment*, 10 (2):147–51.

Iivari, J. and Hirschheim, R. (1996). Analyzing information systems development: A comparison and analysis of eight is development. *Information Systems Journal*, 21(7):551–575.

ISO/IEC (2005). The international standards ISO/IEC. Retrieved March 1, 2007, from http://www.saiglobal.com.

Ives, B., Hamilton, S., and Davis, G. (1980). A framework for research in computer-based management information systems. *Management Science*, 26(9):910–934.

Jennex, M. E., . O. L. (2006). A model of knowledge management success. *International Journal of Knowledge Management*, 2(3):51–68.

Joia, L. (2003). Key success factors for electronic interorganisational co-operation between government agencies. *Proceedings of the 4th IFIP International Working Conference on Knowledge Management in Electronic Government, M.A. Wimmer (Ed.)*, 2645:76–81.

Jones, M. (2007). Hofstede culturally questionable? *Oxford Business & Economics Conference. Oxford, UK*, pages 24–26.

Kanungo, R. N. and Jaeger, A. M. (1990). *Management in Developing Countries.* Routledge, New York.

Kaplan, B. and Maxwell, J. (1994). *Qualitative Research Methods for Evaluating Computer Information Systems in Evaluating Health Care Information Systems: Methods and Applications.* Sage, Thousand Oaks.

Karahanna, E., Straub, D., and Chervany, N. (1999). Information technology adoption across time: Cross-sectional comparison of pre-adoption and post-adoption beliefs. *MIS Quarterly*, 17(2):183–213.

Khalfan, A. and Ashawaf, A. (2003). IS/IT outsourcing practice in the public health sector of Kuwait a contingency approach. *Logistic information Management*, 16(3/4):215–228.

Klein, K. and Myers, D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly*, 23(1):67–93.

Knapp, K., Marshall, T., Rainer, K., and Nelson, F. (2006). Information security: management's effect on culture and policy. *Information Management & Computer Security*, 14(1):24–36.

Koh, K., Ruighaver, A., Maynard, S., and Ahmad, A. (2005). Security governance: Its impact on security culture. *In Proceedings of The third Australian Information Security Management Conference, Perth, Australia;*.

Kowalski, S. (1994). The SBC Model as a Conceptual Framework for Reporting IT Crimes. In *Proceedings of the IFIP TC9/WG9.6 Working Conference on Security and Control of Information Technology in Society on board M/S Illich and ashore*, pages 207–226. North-Holland Publishing Co.

Kuusisto, R., Nyberg, K., and Virtanen, T. (2004). Unite security culture may a unified security culture be plausible? *Proceedings of the 3rd European Conference on Information Warfare and Security (ECIW 2004)*, pages 221–229.

Kuusisto, T. and Ilvonen, I. (2003). Information security culture in small and medium size enterprises. *Frontiers of E-business Research*.

Lam, W. (2005). Barriers to e-government integration. *Journal of Enterprise Information Management*, 18(5/6):511–530.

Levine, J. and Moreland, R. (1999). *Knowledge transmission in work groups: helping newcomers to succeed*, volume Lawrence Erlbaum: Mahwah, NJ, chapter In Shared Cognition in Organizations: The Management of Knowledge, pages 267–296. Lawrence Erlbaum: Mahwah, NJ.

Loch, K., Straub, D., and Kamel, S. (2003). Diffusing the Internet in the Arab World: The Role of Social Norms and Technological Culturation. *IEEE Transactions on Engineering Management*, 50(1):45–63.

Lyytinen, K. (1987). Different perspectives on information systems: Problems and solutions. *ACM Computing Surveys*, 19(1).

Markus, M. and Robey, D. (1988). Information technology and organizational change: causal structure in theory and research. *Management Science*, 34(5):583–599.

Martins, A. and Eloff, J. (2002). Information security culture. *In: IFIP TC11 international conference on information security , Cairo, Egypt*, pages 7–9.

Mason, J. (2002). *Qualitative researching (2nd ed.).* London: Sage Publications.

May, L. and Lane, T. (2006). A Model for improving e-Security in Australian Universities. *Journal of Theoretical and applied Electronic Commerce Research*, 1(2):90–96.

Mendonca, M. and Kanungo, R. (1996). Impact of culture on performance management in developing countries. *International Journal of Manpower*, 17 (4/5):65–75.

Miles, M. and Huberman, A. (1994). *Qualitative data analysis.* Sage, Thousand Oaks, 2nd edition.

Mohannak, K. and Hutchings, K. (2007). *Knowledge Management in developing Economies*, chapter Knowledge Management: Towards A Cross-Cultural and Institutional Framework. Edward Elgar.

Molla, A. and Ioannis, L. (2005). Success and Failure of ERP Technology Transfer: A Framework for Analysing Congruence of Host and System Cultures. *Working Paper Series. Viewed from: http://www.sed.manchester.ac.uk/idpm/publications/wp/di/index.htm*, Paper No 24.

Moon, M. (2000). Organizational commitment revisited in new public management: Motivation, organizational culture, sector, and managerial level. *Public Performance & Management Review*, 24(2):177–194.

Myers, D. (1997). Qualitative Research in Information Systems. Available from: http//comu2.aucland.ac.nz/-isworld/quality.htm. [Accessed 25 March 2007].

Nakata, C. and Sivakumar., K. (2001). Instituting the Marketing Concept in a Multinational Setting: The Role of National Culture. *Journal of the Academy of Marketing Science*, 29(3):255–275.

Nelson, K. (2008). *Information and Knowledge Management (IKM) in Business Contexts*. VDM Verlag Dr.Muller.

Nelson, R. and Gopalan, S. (2003). Do organizational cultures replicate national cultures? *Organization Studies*, 24:1115–1151.

Neuman, W. (1997). *Social research methods: Qualitative and quantitative approaches(3rd)*. Needham Heights, MA: Allyn & Bacon.

Newcomer, E., Caudle, K., and Sharon, L. (1991). Evaluating public sector information systems: More than meets the eye. *Public Administration Review.*, 51(5):377–384.

Ngo, L., Zhou, W., and Warren, M. (2005). Understanding transition towards information security culture change. *In: Proceedings of the third Australian information security management conference, Perth, Australia;*.

Norris, D. and Moon, M. (2005). Advancing e-government at the grassroots: Tortoise or hare? *Public Administration Review*, 65-75(1):64.

Nour, M., AbdelRahman, A., and Fadlalla, A. (2007). A context-based integrative framework for e-government initiatives. *Government Information Quarterly*, 25(3):448–46.

Orlikowski, W. and Baroudi, J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research,*, 2(2):1–28.

Ostroff, F. (2006). Change management in government. *Harvard Business Review*, 84(5):141–147.

Parsons, J. (1996). An information model based on classification theory. *Management Science*, 42(10):1437–1453.

Patton, M. (2002). *Qualitative research and evaluation methods. 3rd ed.* Thousand Oaks, CA: Sage Publications.

Patton, M. Q. (1990). *Qualitative evaluation and research methods.* Sage, Newbury Park, CA: Sage, 2nd edition.

Peterson, M. F. and Smith, P. B. (1997). Does national culture of ambient temperature explain cross-national differences in role stress? no sweat! *Academy of Management Journal*, 40(4):930–946.

Pfeffer and Sutton (2000). *How Smart Companies Turn Knowledge into Action.* Harvard Business Press.

Place, I. (1982). *Records management: controlling business information.* Reston, VI: Reston.

Poortinga, Y. (1992). Towards a conceptualization of culture for psychology. *In S.Iwawaki, Y.Kashima, & K.Leung (Eds.), Innovations in cross-cultural psychology. Amsterdam: Swets & Zeitlinger*, pages 3–17.

Rainey, G. and Steinbauer, P. (1999). Galloping elephants: Developing elements of a theory of effective government organizations. *Journal of Public Administration Research and Theory*, 9(1):1–32.

Ramachandran, S., Rao, S., and Goles, T. (2008). Information security cultures of four professions: A comparative study. *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*, pages 454–454.

Raman, K. and Wei, K. (1992). *The GDSS research project. In R.P. Bostrom, R.T. Watson & S.T. Kinney (Eds.).* Computer Augmented Teamwork: A Guided Tour. New York, NY: Van Nostrand Reinhold.

Recht, R. and Wilderom, C. (1998). Kaizen and culture: on the transferability of japanese suggestion systems. *International Business Review*, 7:7–22.

Reimers, J. and Barbuto, J. (2002). A framework exploring the effects of the machiavellian disposition on the relationship between motivation and influence tactics. *Journal of Leadership & Organizational Studies*, 9 (2):29–41.

Rosacker, K. and Olson, D. (2008). Public sector information system critical success factors. *Transforming Government: People, Process and Policy*, 2(1):60–70.

Ruighaver, B., Maynard, B., and Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security*, 26(1):56–62.

Saint-Germain, R. (2005). Information Security Management Best Practice Based on ISO/IEC 17799. *Information Management Journal*, 39(4):60–66.

Salman, A. (2004). Elusive challenges of e-change management in developing countries. *Business Process Management Journal*, 10(2):140–157.

Schaffer, B. and Riordan, C. (2003). A review of cross-cultural methodologies for organizational research: A best- practices approach. *Organizational Research Methods*, 6(2):169–215.

Schein, E. H. (1985). *Organizational Culture and Leadership.* San Francisco: Jossey-Bass.

Schein, E. H. (2004). *Organizational Culture and Leadership.* Hoboken: John Wiley & Sons, Inc.

Schlienger, T. and Teufel, S. (2002.). Information security culturethe socio-cultural dimension in information security management. *FIP TC11 International Conference on Information Security, Cairo, Egypt; 7-9 May 2002.*

Schlienger, T. and Teufel, S. (2003). Analyzing information security culture: increased trust by an appropriate information security culture. *Database and Expert Systems Applications, 2003. Proceedings. 14th International Workshop on*, pages 405–409.

Scholl, H. (2003). E-government: a special case of ICT-enabled business process change. *System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on System Sciences*, page 12.

Schwandt, T. A. (1997). *Qualitative Inquiry,.* Thousand Oaks, CA: Sage.

Selmer, J. and DeLeon, C. (1996). Parent cultural control through organizational acculturation: HCN employees learning new work values in foreign business subsidiaries. *Journal of Organizational Behavior*, 17:557–572.

Singleton, P., McLean, R., and Altman, N. (1988). Measuring Information Systems Performance: Experience with the Management by Results System at Security Pacific Bank. *MIS Quarterly*, 12(2):325–337.

Siponen, M. (2000a). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1):31–41.

Siponen, M. (2000b). Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice. *Information Management & Computer Security*, 8(5):197–209.

Siponen, M. and Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *SIGMIS Database*, 38(1):60–80.

Smith, E. and Medin, D. (1981). *Categoriesa and Concepts.* Harvard University Press, Cambridge, MA.

Smith, P., Achoui, M., and Harb, C. (2007). Unity and Diversity in Arab Managerial Styles. *International Journal of Cross Cultural Management*, 7(3):275–289.

Smith, P., Peterson, M., and Schwartz, S. (2002). Cultural values, sources of guidance and their relevance to managerial behaviour: A 47 nation study. *Journal of Cross-Cultural Psychology*, 33(2):188–208.

Smith, P. B. (1992). Organizational behavior and national culture. *British Journal of Management*, 3:39–51.

Stake, R. (1995). *The art of case study research.* Thousand Oaks, CA: Sage Publications.

Stanton, J., Stam, M., Mastrangelo, P., and Jolton, J. (2005). Analysis of end user security behaviors. *Journal of Computers and Security*, 24:124–133.

Stewart, J. and Walsh, K. (1992). Change in the management of public services. *Public Administration*, 70(4):499–518.

Stout, A. and Blair, M. (2001). Trust, trustworthiness, and the behavioral foundations of corporate law. *University of Pennsylvania Law Review, June 2001. Available at SSRN: http://ssrn.com/abstract=241403.*

Straub, D., Carlson, J., and Jones, H. (1993). Deterring cheating by student programmers: A field experiment in computer security. *Journal of Management Systems*, 5:33–48.

Straub, D., Loch, K., Evaristo, R., Karahanna, E., and Srite, M. (2002). Toward a theory-based measurement of culture. *Journal of Global Information Management*, 10(1):13–23.

Straub, D., Loch, K., and Hill (2001). Transfer of information technology to the arab world: A test of cultural influence modeling. *Journal of Global Information Management*, 9:6–28.

Straub, D. and Nance, W. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly*, 14:4562.

Sveen, F. O., Rich, E., and Jager, M. (2007). Overcoming organizational challenges to secure knowledge management. *Inf Syst Front*, 9:481–492.

Tarimo, C. (2006). *ICT Security Readiness Checklist for Developing countries: A Social–Technical Approach.* PhD thesis, Stockholm University, Royal Institute of Technology.

Thomson, K., von Solms, R., and Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security*, 10:7–11.

Tyler, T., Callahan, E., and Jeffrey, F. (2007). Armed, and Dangerous (?): Motivating Rule Adherence Among Agents of Social Control. *Law & Society Review.*

UN (2005a). Information economy report 2005. Technical report.

UN (2005b). United nations global e-government readiness report. Technical report, UN.

Van Niekerk, J. and von Solms, R. (2006). Understanding information security culture: A conceptual framework. *In proceedings Information Security South Africa (ISSA), Johannesburg, South Africa.*

von Solms, B. (1999). Information security management: why standards are important. *Information Management & Computer Security*, 7(1):50–57.

von Solms, B. (2000). Information security -The third wave? *Computers & Security*, 19(7):615–620.

von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? *Computers & Security*, 24(2):99–104.

von Solms, B. (2006). Information Security -The Fourth Wave. *Computers & Security*, 25(3):165–168.

von Solms, B. and von Solms, R. (2004a). The 10 deadly sins of information security management. *Computers & Security*, 23(5):371–376.

von Solms, R. (1998). Information security management (3): the Code of Practice for Information Security Management (BS 7799). *Information Management & Computer Security*, 6(5):224–225.

von Solms, R. and von Solms, B. (2004b). From policies to culture. *Computers & Security*, 23:275–279.

Vroom, C. and von Solms, R. (2004). Towards information security behavioral compliance. *Computers & Security*, 23(3):191–198.

Walsham, G. (1993). *Interpreting Information Systems in Organizations.* Chichester, Wiley.

Walsham, G. (2002). Cross-cultural software production and use: A structurational analysis. *MIS Quarterly,*, 26(4):359–380.

Walsham, G. and Waema, T. (1994). Information systems strategy and implementation: A case study of a building society. *ACM Transactions on Information Systems*, 12:150–173.

Ward, J. and Elvin, R. (1999). A new framework for managing IT-enabled business change. *Information Systems Journal*, 9(3):197–221.

Watson, R. T., Kelly, G. G., Galliers, R. D., and Brancheau, J. C. (1997). Key issues in information systems management: An international perspective. *Journal of Management Information Systems*, 13(4):91–115.

Wiander, T., Savola, R., Karppinen, K., and Rapeli, M. (2006). Holistic information security management in multi organization environment. In IEEE, editor, *IEEE ISIE 2006,*, Montreal, Quebec, Canada. IEEE.

Workman, M., Bommer, W., and Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24:2799–2816.

Yavas, U. (1992). Constraints on the application of management know-how in the third world. *International Journal of Management*, 17-25.

Yin, R. K. (2003). *Case Study Research, Design and Methods*. Sage Publications, Newbury Park, 3rd edition.

Zakaria (2004). Understanding challenges of information security culture: a methodological issue. In *the second Australian information security management conference, Perth, Australia; 26 November 2004*.

Zakaria, N., Stanton, J. M., M, S. T., and Sarker-Barney (2003). Designing and implementing culturally-sensitive IT applications: The interaction of culture values and privacy issues in the Middle East. *Information Technology & People*, 16(1):49–57.

Zakaria, O. and Gani, A. (2003). A Conceptual Checklist of Information Security Culture. *in Proceedings of 2nd European Conference on Information Warfare and Security, Reading, UK.*

Zakaria, O., Gani, A., Nor, M. M., and Anuar, N. B. (2007). Reengineering Information Security Culture Formulation Through Management Perspective. *Proceedings of the International Conference on Electrical Engineering and Informatics, Institut Teknologi Bandung, Indonesia June 17-19, 2007*, pages 638–641.

THE INTERVIEW GUIDE

Introduction:

The purpose of this study is to promote a better understanding of key information system management issues related to information security culture in Saudi Arabia context. This purpose has two primary motivations. The first is to provide organization information technology (IT) managers a useful, integrated, practice-oriented and theoretically sound framework that will assist organizations to succeed in the challenging task of implementing quality information security culture that required to e-government program. Second, to offer information system (IS) academics topics that can provide direction to future research.

The purpose of the interview is to elicit managers and IT staff perspectives about several IT management issues in your organization. Information presented by interviewees will only be used for the purpose of this research. In the description of results of this survey no identification of individual persons will be made. Individual answers will be kept confidential, i.e. the answers will be analyzed, consolidated and presented by category of staff and organizations.

Demographics Questions:

Job title/level:.........................

Education:.........................

Department: ....

Part (1): Contains structured questions about current information security practices.

1. **What do you consider to be the top three main causes of security incidents in your organization?** ***Please select three***

   □ Viruses and malicious software

   □ System or software errors

   □ Cyber or internal based attacks

   □ User's errors or non compliance

   □ System administrator's errors or non compliance

   □ Hardware failure

   □ Other (please specify)

2. **In your view, what do you consider to be the top three barriers or obstacles to achieving improved security compliance?** ***Please select three***

   □ Lack of awareness and training programs

   □ Lack of inadequate technology

   □ Clear direction in security procedures and roles

   □ Lack of motivation programs

   □ Other (please specify)

3. **Can you rank order the following influences on security-related behaviors?**

   □ IT Department initiatives in your organization (e.g. policies, guidelines, procedures, training programs, rewards, and penalties)

   □ Personal culture (i.e. values and beliefs) about information security

   □ Information security technical countermeasures (e.g. Anti-virus software, firewall, intrusion detection..)

   □ Top management commitment (e.g. management gives strong consistence support to security programs, budget is allocated to information security programs)

4. **Please choose the answer that best reflects your opinion about the entire organization (company) that you work for.**

   Yes = indicates the practice is implemented.

   Partially = indicates that part of the practices is implemented.

   No = indicates the practice is not implemented at all.

Yes	**Partially**	**No**	**Items**
			Management commitment:
[ ]	[ ]	[ ]	Top management considers information security an important organizational priority.
[ ]	[ ]	[ ]	Top management gives strong and consistent support to the security program.
			Security compliance:
[ ]	[ ]	[ ]	There is a clear procedure to discipline members who violate organizational security policy and regulations.
[ ]	[ ]	[ ]	Information security rules are enforced by all managers.
[ ]	[ ]	[ ]	Password sharing among users is an issue in your organization.
[ ]	[ ]	[ ]	Your organization routinely conducts information security audits and maintains historical records/data of information misuse or intrusion attempts.
			Awareness:
[ ]	[ ]	[ ]	There are appropriate awareness programs to ensure that members of the organization are aware of their security responsibilities (ex. training sessions/workshops on security organized).
[ ]	[ ]	[ ]	Members of your organization take IS courses as part of their education.
			Skills and training:
[ ]	[ ]	[ ]	There is a regular and structured training program to all members on information security.
[ ]	[ ]	[ ]	There are adequate in-house expertise for all supported services, mechanisms and technologies.
			IS structure:
[ ]	[ ]	[ ]	Your organization has a strong hierarchical structure.
[ ]	[ ]	[ ]	IT staff are authorized to make important decisions related to information security issues.

Part (2): Contains open-ended questions for exploring the implementation and the user behavioral pattern related to the information security management.

1. Do you think personal culture (i.e. values and beliefs) influences the security related behaviors?

   □ If YES, have these values and beliefs affected your staff's security-related behaviors? If so, in what aspects? Can you provide examples?

   □ If NO, can you expand?

2. Do you think information security related behaviors of members of the organization has been influenced by the managerial security initiatives like policies, guidelines, procedures, training programs?

   □ If YES, on what ways has it affected your staff's adherence to information security policy?

   □ If NO, what makes you think so?

3. What is your view on the quality of cooperation/communication your organization has with the: a) users and b) with the top management?

4. Do you believe that members of your organization share information and knowledge with IT staff and other colleges voluntarily?

- □ If YES, what are the factors that most influences this to happen in your department?

- □ If NO, what are the factors that most influences this not to happen in your department?

5. When it comes to making decision what level of guidance do IT staff need from upper management?

   - □ Can you comment on the procedures of action when security issues arise?

   - □ When the rules are not clear with respect to information security, or if there is no rule for a situation with respect to information security, how would that be handled by your department? Can you provide examples?

6. Do you believe the information management standards serve a useful purpose in managing your information security effectively?

   - □ If YES, how?

   - □ If NO, why?

7. What motivates the members of your organization to comply with information security policy?

8. How do tangible rewards (such as money, promotion) compare to intangible rewards (such as satisfaction and appreciation)

9. Can you comment on the procedures of action when resistance to security measures has come about?

10. What other specific information security related issues and factors do you see and encounter in terms of the effectiveness of the information system in your organization?

Letter to Participants

Dear ....

I am carrying out a research at the Queensland University of Technology (QUT), focusing on potential solutions in relation to e-government management of Information security. As part of the research, your organization has been chosen as one of three organizations in the Kingdom of Saudi Arabia to participate as a case study. Particularly, ITC staff experience in the issues related to e-government security at your organization.

Please spend a few minutes going through the introduction section to get an overview and objective of this research.

Information presented by interviewees will only be used for the purpose of this research. In the description of results of this survey no identification of individual persons will be made. Individual answers will be kept confidential, i.e. the answers will be analyzed, consolidated and presented by category of staff and organizations.

Thank you in advance for your valuable time and consideration.
Kind Regards,

Salahuddin Alfawaz
Phd. Student, ISI
Queensland University of Technology
Brisbane, Australia
E-mail: s.alfawaz@student.qut.edu.au

Coding Mechanism

Overview of Coding Procedures:

The research data was collected from thirty eight participants from three cases in Saudi Arabia. The notes of the interviews were taken on paper and most of them were recorded. After each interview, the notes of each interview were entered in the research database. They were then assigned a code. The coding mechanism is structured as follows: a digit number to represent the participant number and a single character to designate the case. For example, P4-A represents a quot of participant number 4 from Case A. The same process was repeated for all the notes of the participants in all three cases.

The categories coding involves the following steps:

- Defining the Coding Categories. In the analysis stage, data from all of the resources were continuously re-examined and presented under these six themes:

  1. Influence of national culture values
  2. Influence of organisational values
  3. Influence of technology
  4. Practices
  5. Outcomes
  6. Change management

- Once the set of coding categories is developed and defined, we assigned a unique code for each category (see Table 1. Then we assign an abstract symbol to represent any case in that category. Thus each category has its own code.

- Then we highlight the relevant themes, words and phrases. Figure 3 shows an example of this step.

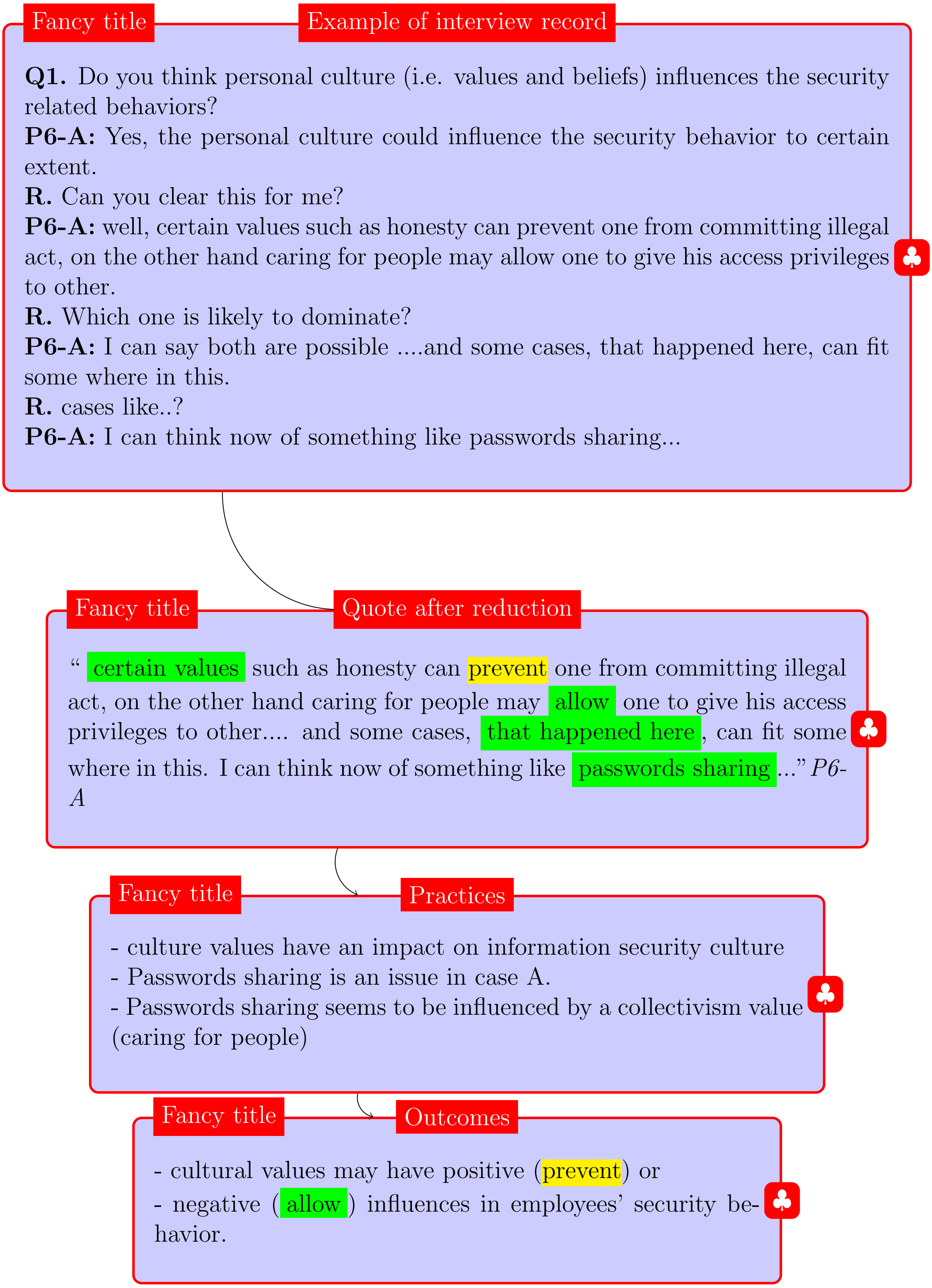
- To store each fragment of relevant information into the appropriate location, we use a coding sheet in which the column and row headings represent the categories of relevant information we have defined (see Table 2).

Table 1: Example of Category Codes

Code	**Description**
Inf-NC-BSC	Influence of National Culture values on members' behavior related to information security culture.
Inf-PD-BSC	Influence of Power distance on members' behavior related to information security culture.
Inf-UA-BSC	Influence of Uncertainty Avoidance on members' behavior related to information security culture.
Inf-IC-BSC	Influence of Individualism vs Collectivism on members' behavior related to information security culture.
Inf-CC-BSC	Influence of Context (Communication) on members' behavior related to information security culture.
Inf-OC-BSC	Influence of Organizational Culture values on members' behavior related to information security culture.
Inf-TM-BSC	Influence of Top Management's commitment on information security culture.
Inf-ISS-BSC	Influence of IS Structure on members' behavior related to information security culture.
Inf-TS-BSC	Influence of training and skills on members' behavior related to information security culture.
Inf-AW-BSC	Influence of Awareness programs on members' behavior related to information security culture.
Inf-MM-BSC	Influence of Motivation Mechanisms on members' behavior related to information security culture.
Inf-MA-BSC	Influence of Managerial security Activities on members' beliefs related to information security culture.
Inf-TC-BSC	Influence of information security Technical countermeasures on members' behaviors' related to information security culture.
Inf-OF-BSC	Influence of Organizational Factors on members' behavior related to information security culture.
Inf-SE-BSC	Influence of information Security Events on members' behavior related to information security culture.
Inf-OE-BSC	Influence of Organizational Events on members' behavior related to information security culture.

Table 2: Example of interview record

Influence of Values	Participant	Example of interview	Practices	Outcomes
Inf-TM-BSC	P3-C	“ top management support was very important for us at the start of our program... and I think we need more from them to keep things run smoothly”	-Management support at the start of our program -A need for consistency	Activities related to IT support might not run smoothly
Inf-ISS-BSC	P2-C	“we all serve one goal, but when it comes to responsibility one should know his won boundaries,... and clearing this issue allows our staff to know their territory and avoid possible overlap of such responsibility. ”	-Overlap of responsibility over IT security -Tension, conflict	
Inf-TS-BSC	P4-C	“Although we don’t have comprehensive security initiatives, but some initiatives have impacted security related behavior such as awareness and training. There is a need to enhance the awareness of security issue and how much crucial it is for our information security ”	-No structure programs. -There is a need to enhance	-some initiatives impacted security related behavior
Inf-AW-BSC	P7-A	”the IT department send a lot of warning e-mails related to security issues...almost every day...but I’m sure not every one take them seriously.”	-E-mail used as a medium to raise Awareness -Too many warning e-mails	-not every one takes them seriously



Fancy title

Example of interview record

Q1. Do you think personal culture (i.e. values and beliefs) influences the security related behaviors?
P6-A: Yes, the personal culture could influence the security behavior to certain extent.
R. Can you clear this for me?
P6-A: well, certain values such as honesty can prevent one from committing illegal act, on the other hand caring for people may allow one to give his access privileges to other.
R. Which one is likely to dominate?
P6-A: I can say both are possible ....and some cases, that happened here, can fit some where in this.
R. cases like..?
P6-A: I can think now of something like passwords sharing...

Fancy title

Quote after reduction

" certain values such as honesty can prevent one from committing illegal act, on the other hand caring for people may allow one to give his access privileges to other.... and some cases, that happened here, can fit some where in this. I can think now of something like passwords sharing..." *P6-A*

Fancy title

Practices

- culture values have an impact on information security culture
- Passwords sharing is an issue in case A.
- Passwords sharing seems to be influenced by a collectivism value (caring for people)

Fancy title

Outcomes

- cultural values may have positive (prevent) or
- negative (allow) influences in employees' security behavior.

FIGURE 3: Example of highlighting the relevant themes, words and phrases.