2009

Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context

Mohammed Alnatheer
Queensland University of Technology

Karen Nelson
Queensland University of Technology

DOI: 10.4225/75/579850d331b4d
Originally published in the Proceedings of the 7th Australian Information Security Management Conference, Perth, Western Australia, 1st to 3rd December 2009

A Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context

Mohammed Alnatheer[1] & Karen Nelson[2]
Information Security Institute
Queensland University of Technology

[1] mohammed.alnatheer@student.qut.edu.au
[2] kj.nelson@qut.edu.au

Abstract

An examination of Information Security (IS) and Information Security Management (ISM) research in Saudi Arabia has shown the need for more rigorous studies focusing on the implementation and adoption processes involved with IS culture and practices. Overall, there is a lack of academic and professional literature about ISM and more specifically IS culture in Saudi Arabia. Therefore, the overall aim of this paper is to identify issues and factors that assist the implementation and the adoption of IS culture and practices within the Saudi environment. The goal of this paper is to identify the important conditions for creating an information security culture in Saudi Arabian organizations. We plan to use this framework to investigate whether security culture has emerged into practices in Saudi Arabian organizations.

Keywords
Information security management, Information security policy, Information security compliance, Information security risk analysis, Information security awareness and training programs, Security culture, Organizational culture, National culture

INTRODUCTION

Information security may be defined as the prevention of, and recovery from, unauthorized or undesirable destruction, modification, disclosure, or use of information and information resources, whether accidental or intentional. According to Pfleeger (1997), information security is the preservation of the confidentiality, integrity, and availability (CIA) of information and information resources. Information security maintains three basic services:

1. Confidentiality of sensitive information, which is concerned with preventing disclosure of information to unauthorized users.
2. Integrity, which is concerned with ensuring data cannot be modified without authorizations.
3. Availability, which is concerned with ensuring information must be available to authorized users when they require them (Pfleeger, 1997).

ISM focuses on developing and maintaining quality information infrastructures. ISM enhances the confidence and effectiveness of information services within an organization, or between an organization and its external business partners (von Solms, 1996). The overall goal of ISM is the prevention or minimization of damage to organizational assets. ISM can enhance organizations' performance, and its establishment is fast becoming the normal way of doing business and effective ISM ensures business continuity (British Standards Institution, 1995). Globalization and international competition increases the importance of ISM (von Solms, 1999, 2000). In recent years, several countries (e.g. the USA, the UK, China, and others) have made investments to establish basic information security techniques (Rathmell, 2001). In developed countries, IS cultures and practices occur because of the recognition of the importance of IS and its influence on their economies. According to an Ernst and Young survey, security incidents can cost companies between $17 and $28 million (Garg, Curtis & Halper, 2004). The impact of security breaches and attacks on organizational prosperity includes loss of reputation, financial loss and business confidences. Therefore organizations in developed countries work to ensure a secure environment for their information and communication technologies (ICT) to safeguard performance and productivity.

However, the majority of the research about ISM has been performed by technologically leading countries such as the United States of America, the United Kingdom, the European Union and Australia. Saudi Arabian information technology capacities are still in a developmental phase and are immature in relation to leading western technologically developed countries. So while information security and its management are concerned with people, processes and technology and the technology itself can be seen as relatively objective by nature; the people and processes are influenced by the environment in which they operate. The business environment of Saudi is different to the business environment in the USA and other Western countries. Furthermore, information security major international standards

are written from a Western perspective, without knowing how applicable ISM concepts and practices are to other cultures, in this case, Saudi Arabia. As a result, there may be a need for extra or different considerations for ISM implementation in non-Western environments including Saudi Arabia. We propose that these considerations are likely to be related to culturally distinct issues in the Saudi context.

Developing countries such as Saudi Arabia have invested in creating and building ICT infrastructures, but the cultural differences in Saudi, compared to western developed countries in terms of IS culture and practices is thought to be a challenging ISM implementation issue for the Saudi organizations. Therefore, this paper proposes a conceptual framework that can be used to identify and investigate the factors that will lead to success in terms of implementing and adopting IS culture and practices in Saudi Arabia. We contend that this framework will assist in addressing the two gaps in current ISM research already identified in this paper. Firstly this examines ISM from the perspective of Saudi Arabian organizations and addresses the paucity of academic and professional research about IS culture and practices in Saudi Arabia. Secondly, there is a need to define what ISM factors must be present in order to have effective IS culture and practices. Therefore this paper addresses this gap by developing a framework that identified the ISM factors and the cultural factors that are understood to aid the implementation and the adoption of IS culture and practices in Saudi environment.

The following topics are covered in the remainder of this paper. Section two provides a context for our work by describing the Saudi Arabia context. The third section discusses security cultures. Then, this paper discusses the factors and issues influencing IS cultural and practices and the conceptual framework development. Finally, this paper finished by presenting a brief conclusion and future work for this study.

INTRODUCTION TO THE SAUDI ARABIA CONTEXT

Saudi Arabia has population of 27 million of which 60 % are under the age of 25 and 40 % of the population are under 15 (Ministry of Planning, 2009). The population is expected to reach nearly 40 million by 2025 (Mouawad, 2008). Saudi Arabia is considered to be a developing country. The World Bank, (2009) defined developing countries as Countries that are below- or middle-income countries compared with developed countries, and where living standards are thought to be low relative to high-income countries. Developing countries have low standards of living and a low industrial capacity (World Bank, 2009). Despite this status, Saudi Arabia is the largest economy in the Middle East, comprising 25% of the Arab world's GDP (USSABC, 2008). It is the world's leading oil exporter, possessing one-fourth of the world's proven oil reserves (Energy Information Administration, 2009).

For more than 35 years, Saudi Arabian economic development has been broadly governed by five-year economic development plans. The latest plan (8th Plan) was approved in November 2005 (USSABC, 2008). Previous plans drove ICT development between 1990 and 2000 and emphasized the improvement of education, financial, legal and technical skills to create private sector employment opportunities for Saudi citizens (Background Note: Saudi Arabia, 2009). The overall purpose of the economic plans is to reduce the dependency of the country's economy on the oil sector by diversifying economic activity through encouraging growth in the private sector. The current 8th plan (2005-2010) continues to focus on economic diversification, increasing expenditure on education, ICT, legal regulations and healthcare (Background Note: Saudi Arabia, 2009). The Saudi government's objective is to promote public services, achieve prosperity for society, raise the productivity of all sectors, and consequently raise the Gross Domestic Product (GDP). The improving business environment, boosted by privatization and liberalization, is providing the Saudi economy an advantage in terms of attracting foreign investors into the country.

The Saudi government aims to make the country one of the top ten world destinations, in terms of investment competitiveness, by 2010 (Saudi Arabian General Investment Authority, 2009). Currently, Saudi Arabia is ranked number 23rd in terms of investment competitiveness (Saudi Arabian General Investment Authority, 2009). The Saudi Arabia economic strategy seeks to encourage regional diversification, foreign direct investment, private sector involvement, and the introduction of knowledge-based industries in Saudi Arabia (Saudi Arabian General Investment Authority, 2009). Implementation of the new strategy will support for the development of industrial and technology clusters; support for SMEs with incubator programs and business resource centers, and improved industrial financing mechanisms; programs to boost national and regional innovation, and programs to enhance industrial cluster–related human resource capabilities (Saudi Arabian General Investment Authority, 2009).

Saudi Arabia also developed a National Communications and IT Plan (NCITP) in 2005 as part of the 8th economic development plan. The NCITP is composed of two components;

- A five-year plan for Communications and IT in the country.
- A long-term perspective for Communications and IT in the country.

The five-year plan is a progression towards the long-term perspective. The long-term vision for ICT in the country of Saudi Arabia is: "The transformation into an information society and digital economy so as to increase productivity and provide communication and IT services for the sectors of the society in all part of the country and build a solid a information industry that becomes a major source of income" (Ministry of Communications and Information Technology, 2006).

Information security and its management are essential parts of the ICT infrastructure required to support the development of the Saudi Arabia economy. Lack of a mature approach to ISM could cause significant damage to Saudi organizations and the national economy. To address this; the Saudi government has encouraged the establishment of secure environments in both sectors (public and private) (Ministry of Communications and Information Technology, 2006). It has also established ICT infrastructures to increase the productivity and performance of organizations and individuals in Saudi Arabia. As a result, adopting an IS culture and practices within Saudi organizations is a major challenge to be dealt with to protect their economic assets from attacks and intruders. The next section discusses the factors and issues that need to be considered to maximize ICT benefits in any organizations.

SECURITY CULTURE

Literature in the area of security shows that research on information security culture is still in its early stages of development. Issues are still being identified, and, conceptualizations being explored. Culture has influenced the formation of many security measures, such as national security policy, information ethics, security training, and privacy issues (Chen, Medlin, & Shaw, 2008). Security culture covers social, cultural and ethical measures to improve the security relevant behavior of the organizational members and considered to be a subculture of organizational culture (Schlienger & Teufel, 2002). Security culture should support all organizational activities in a way that information security becomes a natural aspect in the daily activities of every employee (Schlienger and Teufel, 2002, p. 197). Security cultures assist the enforcement of information security policies and practices to the organization. As a result, each organization goal's is to be able achieve an effective information security culture in their organization. Information security culture will emerge over time and become evident in the behavior and activities of the workforce (da Veiga, Martins, & Eloff, 2007).

Recent studies have shown that the establishment of an organizational information security culture is necessary for effective information security (Eloff & Von Solms, 2000; Von Solms, 2000). However, organizational culture may have a substantial influence on the security of information, and this could be negative or positive (Chang, & Lin, 2007). It is imperative that the organizational culture reflects a positive attitude to information security in the entire organization (Schlienger & Teufel, 2003; Zakaria, Jarupunphol, & Gani, 2003; Vroom, R. von Solms, 2004) and it is also important that organizational activities are consistent with good information security culture practices (van Niekerk, and von Solms, 2005). On the other hand, (Chia, Maynard, and Ruighaver, 2002), argue on the importance for organization to assess their security culture, and organization management must focus to establish security culture within the organization culture (Ruighaver, Maynard, & Chang, 2007).
There is a little agreement on security culture definition or what exactly constitutes security culture (Ruighaver, et al., 2007). The majority of research on security culture promotes the benefits of security culture without providing supportive evidence. As a result, there is little empirical work that investigates the relationship between security culture and ISM factors in addition to cultural factors. The current study attempts to fill this gap and contribute to the behavioral information security literature by exploring the influence of ISM factors and cultural factors towards the implementation and the adoption of security culture. This study is mainly interested on understanding the critihcal factors influence security culture so it would assist organization to be able to adopt security culture as a normal behavior in their organization. In the next section we review the factors that may aid in the implementation and adoption of IS culture and practices in the Saudi context.

FACTORS AND ISSUES THAT INFLUENCES SECUIRTY CULTURE AND PRACTICES

This section examines the ISM factors, and a cultural issue that may influence IS culture and practices in Saudi Arabia environment. The literature drawn on for this analysis has largely been sourced from work investigating IS culture and practices in developed countries such as the USA, the UK, and Australia, and we use them as a guideline for identifying IS cultural and practices in Saudi Arabia. A comprehensive search of the academic literature was conducted to identify papers and an article published about ISM and IS culture in the ten year period between 1998 to 2008 to identify the issues and factors that influence IS culture and practices in the literature. This search identified 100 ISM and IS culture related papers. 68 of these papers were found to focus specifically on identification or investigation of the factors that aid the implementation and the adoption of IS culture and practices. Of these papers 28 (41%) had an empirical analysis that included data gathering and analysis. The remaining 40 (59%) of these papers focused on presenting ISM frameworks or reviewing ISM issues and factors already present in the literature. Our analysis showed that 27 of the empirical papers referred to studies that had been conducted in developed countries such as the USA, UK, Australia, Europe, Taiwan and South Korea. Only one paper appeared to be based on research conducted in a developing country (the United Arab

Emirates). This quick analysis indicated a real gap in knowledge in terms of ISM studies in developing countries. The literature analysis could not identify any papers that included holistic frameworks or articulated a complete model showing all the factors that aid the implementation and adoption of IS culture. However the 68 papers did reveal a range of issues and factors that influence IS culture and practice. These factors included: Information Security Awareness, and Training Programs, ISM Standardization, Information Security Policy, Top Management Support for ISM, Information Security Compliance, Information Security Risk Analysis, and Organizational Culture. These issues were classified into the following themes, each of which is discussed further below:

- Corporate citizenship
- Legal regulatory environment
- Corporate governance
- Cultural factors

However, in the case of Saudi Arabia, national cultural factors tend to be obstacles and can affect the adoption of IS cultural and practices in Saudi Arabian organizations. Therefore, this study will examine the influence of ISM factors and cultural factors on the adoption of IS cultural and practices in Saudi Arabia.

Corporate Citizenship

Information Security Awareness and Training Programs

The theme of corporate citizenship is concerned with how employees gain an understanding of appropriate IS culture and practice through awareness raising and training programs. The notion of corporate citizenship is applied at three levels (national, organizational, and individual). Senge (1990) refers to information security awareness as a state where users in an organization are aware of, and ideally committed to, their security mission. Information security awareness is important part of ISM (Nosworthy, 2000; Schultz, 2004; Thomson and Von Solms, 1998). Increasing awareness of security issues is the most cost-effective control that an organization can implement (Dhillon, 1999). Hinde, (2002) however suggests that the absence of awareness programs indicate a critical gap in effective security implementation. Security training and awareness programs are therefore a fundamental component of effective information security strategy. Security awareness and training can help organizations to minimize some of the damage caused by misused or misinterpreted application procedures (Straub, 1990; Ceraolo, 1996; Straub and Welke, 1998).

A global information security survey report of 450 information security officers and IT directors (Ernest & Young, 2002) showed that less than 50 percent of employees had received information security awareness training programs. In 2002, a security awareness index survey which was conducted by Pentasafe Security Technologies Inc has published a report based on the results of a free online survey designed to measure organizations' awareness of information security from 583 companies and 1350 individual employees around the world. The survey found 66% of security managers think that information security awareness is inadequate or dangerously inadequate, 50% of employees have never received formal information security training, 10 percent of employees have never read their company security policy, and 25% of employees have not read their security policy in the last two years (Security Awareness Index Survey, 2002). Also, according to Deloitte, Touche, and Tohmatsu, (2005), about 45% of global organizations do not sensitive their employees in respect of possible information security threats, and this lack of information security awareness could well lead to compromised information within the organization. Mitchell, Marcella, and Baxter (1999) found that information security awareness was concentrated around the IT department and did not extend to IT users. There can be major problems if organizations do not realize the importance information security awareness amongst users (von Solms, S.H. & von Solms, R., 2004). Ernst and Young (2001) and Siponen (2000) found that employee awareness is one of the greatest challenges that organizations must face in order to achieve their required level of security. However, one of the least expensive and most practical solutions to ensuring the information security awareness is to provide staff training or development programs to employees.

Legal and Regulatory Environment

In developing countries such as Saudi Arabia, the regulatory and legal environment relating to ICT is still developing. However, the main components of the regulatory and legal environment can be identified from the literature and these are: ISM standardization and best practices, and the presence of information security policies.

Information Security Management Standardization and Best Practices

International best practices for ISM are based on the combined experiences of several influential international companies concerning the way in which they manage their information security (von Solms, 2001). ISM standards are used to establish and maintain a secure environment for information. ISM standards help senior management to monitor and control their security, thus minimizing any residual business risk and ensuring that security continues to fulfill corporate, customer, and legal requirements (How to 27000 Works, 2009). For many years, ISM standards have provided an authoritative statement on the organizational needs for information security and procedures for establishing a security

baseline in organizations (Kwok, 1999). Because an organization's information security can affect their business partners, partners must demand a high level of information security from one another (von Solms, 1999, 2000). ISM standards can give customers and business partners the assurance that services are provided in a secure way, and can increase customer confidence in their business as well as businesses confidence in the organization's business systems (Eloff, & von Solms, 2000) and (Eloff, J., & Eloff, M., 2003). The most common ISM standards that are used and implemented in organizations across the world are ISO 27002, COBIT, OCTAVE, and ITIL. These are not discussed here because of space constraints.

Information Security Policy

The primary objective of information security policy is to define the users' rights and responsibilities in terms of information within an organization (Hong, Chi, Chao, & Tang, 2006). Effective information security policies will help users understand what is acceptable and responsible behavior in information resources and will assist in establishing a safe information environment (Höne & Eloff, 2002). Information security policy is an essential part of security practices within organizations and could substantially influence on their organizational security. As Higgins (1999, p.1) notes, "Without a policy, security practices will be developed without clear demarcation of objectives and responsibilities", and will be face major difficulties when implementing ISM System effectively in their organizations' infrastructures. As a result, organizations cannot achieve effective ISM system without the establishment, implementation, and maintenance of an information security policy (Hong, Chi, Chao, and Tang, 2003). In addition, the formulation and utilization of information security policy can enhance the effectiveness of ISM system (Fulford, 2003). However, even though some organizations have established information security policy, it does not ensure that employees will necessarily obey these policies (von Solms, R., & von Solms, S.H. 2004). As a result, policy enforcement is necessary and essential for the organizations' success. Also, there is a need for organizations to ensure their information security policy is structured and organized effectively (von Solms, R., & von Solms, S.H. 2004).

Corporate Governance

The third theme, corporate governance, includes factors and issues related to top management support for ISM, information security compliance, and information security risk analysis

Top Management Support for Information Security Management

Top management support is seen as the most important factor affecting ISM activities in organizations (Fourie, 2003). In studies by Knapp, Marshall, Rainer, and Morrow (2004, 2007) top management support was ranked number one in a list of 25 security issues affecting information security in organizations. Other bodies, such as the British Standards Institute (1999), support the argument that top management support for ISM is crucial, particularly for implementing information security policy. The British Standards Institute (1999) emphasizes that visible commitment from management and a good understanding of security requirements is key factors affecting the success of the ISM. Support from executive management not only influences uptake of affects information security policy but is also necessary for promoting appropriate ISM activities including: information security awareness and training programs, information security compliance, information security risk analysis, and ISM standardization. A lack of commitment from senior management is a major issue that organizations face in their ISM operations (von Solms, 1996) and may often be found in organizations having difficulties managing their information security.

Information Security Compliance

Compliance processes help organizations compare their actual information security operations with international ISM standards (Karabacak & Sogukpinar, 2006). Compliance evaluates and audits the difference between the expected standards of organizational situations, and the reality in the organization (Karabacak & Sogukpinar, 2006). Evaluating the degree of compliance helps organizations determine their conformity to the controls listed in the standards, and delivers useful outputs to the certification process for the next stage of ISM certification (Karabacak & Sogukpinar, 2006). Compliance with internationally recognized standards is growing in importance, because it has become popular as a common basis for information security measurement (Karabacak & Sogukpinar, 2006).

It is therefore important for organizations to be able to evaluate their information security compliance level (Karabacak &Sogukpinar, 2006; Luthy & Forcht, 2006; Saleh, Alrabiah & Bakry, 2007). Compliance levels increased in organizations that were more aware of their ISM issues, which could lead to improved information security policy and business continuity plans in their organizations (Smith, Jamieson, and Winchester, 2007). Unfortunately, many organizations cannot distinguish between information security compliance management and information security operational management (von Solms, 2005). There have always been problems for organizations in term of information security compliance, which is an obstacle that needs to be overcome in order to achieve the benefits of ISM. As a result, there is a need to find a method to ensure that the practices of employees are compliant company information security policies (Vroom, R. von Solms2004), particularly because a significant number of security breaches result from employees' failure to comply with security policies (Beautement, Sasse, and Wonham, 2008). Many organizations have tried to change or influence security behavior, but found it a major challenge (Beautement, et al., 2008).

Information Security Risk Analysis

Risk is "the likelihood that a threat materializes" (Turban, McLane & Wetherbe, 1996, p.70). To some degree risk is unavoidable and organizations must accept a degree of risk. Caelli, Longley and Shain (1989, p. 417) define risk analysis in the context of risk management in the following way: "The minimizing of risk by effectively applying security measures commensurate with the relative threats, vulnerabilities and values of the resources to be protected. The value of the resources includes the influence on the organization, the automated system supports, and the influence of the loss or unauthorized modification of data".

For many years, risk analysis was regarded as the main method for determining threats and selecting measures for the process of securing computer assets. Information security risk analysis is designed for identifying and assessing the risks for physical assets (Gerber, von Solms, & Overbeek, 2001; Gerber and von Solms, 2005). Information security risk can be thought of as a tradeoff with the corresponding costs of protection. It is important to have an economic evaluation of the security investment to avoid the costs and risks of a security breach (Tsiakis, & Stephanides, 2005). Similarly, it is also very important to find the balance between the economic losses of information security breaches and cost of investment in information security (Finne, 1998). In some countries such as the USA, the UK, Australia, and South Africa, organizations are under constant pressure from government and industry to implement risk management methods (King Committee, 2002). It is almost impossible to determine how much security an organization needs to keep their systems safe from intrusions and in some cases, information security risk analysis raises more questions than they answer (Kwok, 2009). Nevertheless, the benefits of an information security risk method play a very important role in an organization's success. Information security risk analysis can help organizations to measure their economic loss due to problems occurring in their information security processes (Finne, 1998). Information security risk analysis provides organizations with increased knowledge and more depth of understanding regarding their expected loss due to security failure (Gerber, von Solms, & Overbeek, 2001). Information security risk management methods such as CRAMM, CORAS, and OCTAVE help organizations to manage their security exposure (Albert & Dorofee, 2003; ISACA, 2009). Each of these methods has a different approach to identifying, measuring, controlling, and monitoring the information security risk. Organizations must ensure that the information security risk methods methodology employed corresponds with international best practice and is appropriately adapted to their particular environment (Albert & Dorofee, 2003; ISACA, 2009).

Cultural Factors

The fourth theme includes issues related to adopting an IS culture that are related to aspects of national and/or organizational culture. This theme is central to our work because we contend that the context within which organizations in Saudi Arabia operate is different to that experienced by western developed countries (where most previous ISM research has been located) therefore necessitating a consideration of context-sensitive ISM factors and issues.

National Culture

In developing countries such as Saudi Arabia, national culture might have significant impact on the implementation of any new technology or system. Information security is no different to any other technology. However, because no previous research could be found that has investigated the influence of national culture on IS culture and practices in developing countries, our future study will investigate the influence of national cultural factors on the adopting of IS culture and practices in the Saudi environment. The most common national cultural model is Hofstede's (2001) framework which is described briefly below and before being incorporate into the conceptual framework.

Hofstede's Dimensions

According to Hofstede's 1997 study, national culture affects an organization's performance and it is therefore an important consideration when implementing a new practice or system. Sengun and Janell (2003) stated that national culture "remains a significant factor in the acceptance of new products". Our purpose is to investigate the culture of Saudi Arabia and its influence on IS culture and practices in the Saudi environment, using Hofstede's (2001) framework Hofstede (2001) classifies national culture into five dimensions: 1) power distance, which is a measure of the equitable distribution of power; 2) uncertainty avoidance, which is a measure of degree to which cultural members are threatened by uncertain risks; 3) individualism, which is a measure of the balance between tasks over relationships; 4) masculinity, the degree to which social roles are separated on a gender basis; and 5) long-term orientation, which means the degree of traditions in a specific culture and to what extent these traditions are connected to their past and future.

Finestone & Snyman (2005) state that ignoring cultural differences is a serious issue that might cause misunderstandings in which conflict might occur between individuals. Many business leaders consider organizational culture to be independent of national culture, however, Hofstede's (1984) argued that organizational cultures are nested within a national culture, and that national culture influences human resource practices and organizational behavior.

Some studies such as those reported by Bjerke and Al-Meer (1993) and Chadhar and Rhamati (2004) revealed that Saudi Arabia measures high on the following scales: power distance, uncertainty avoidance, high collectivism (low

individualism), and femininity (low masculinity), which indicates that Saudi society has lower chances in implementing and adopting new practices in their culture. Idris (2007) confirms that national culture in Saudi Arabia remains the main challenge for organizations to transforming their local employees into a competitive advantage. On the other hand, Hill, Loch, Straub and El-sheshai, (1998) found that Arab countries are capable of adopting a new technology within their culture despite the challenges and difference in the national culture. Loch, Straub, and Kamel (2003) identified how culture can both inhibit and encourage technological innovation and how Arab cultures can move their economies more quickly into the digital age.

While most research has concentrated on international organizations in developed countries such as the US, the UK, Australia, and Europe, little is known about the particularities of ISM in the developing countries. This is ironic because many organizations are considering relocating their business to developing countries in the longer term (Voelpel & Han, 2005). In particular, the Saudi Government is actively pursuing international and new companies and investments as part of its economic plan (Ministry of Communications and Information Technology, 2006). These international organizations and investors will require that Saudi employees have the capacity to deploy new technologies, especially those that secure ICT infrastructure and other valuable organizational assets. However, previous studies by Bjerke &and Al-Meer (1993), Chadhar and Rhamati (2004), and Idris (2007) all indicate that the implementation and adoption process of new technology such as ISM in Saudi Arabia faces cultural barriers which may negatively influence the implementation and the adoption process within the Saudi society. As a result, there is a need to investigate the influence of national culture on the implementation and adoption of IS culture and practices development within the Saudi Arabian organizations.

Organizational Culture

Organizational culture defines how an employee sees the organization (Schein, 1999). It is a collective phenomenon that is grows and changes over time and, to some extent; it can be influenced or even designed by management. Schein (1999) defines organizational culture as: "the pattern of basic assumptions that a given group has invented, discovered, or developed in learning to cope with its problems of 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 those problems".

For some, culture is the single most important factor accounting for success or failure in an organization (Deal and Kennedy, 1982). However, it has been found that only 5% of organizations have a definable culture, where senior management have taken an active role in the shaping of the corporate culture (Atkinson, 1997). If management does not understand the culture in their organization, it could prove to be fatal in today's business world (Hagberg Consulting Group, 2002). Nevertheless, each organization's corporate culture determines the behavior of its employees (Thomson & von Solms, R. 2006; Schein, 1999), and influences how employees determine acceptable behavior within their organizations (Beach, 1993). Schein (1999, p. 15) cautions that oversimplifying the concept of culture is the biggest danger to understanding it and proposed that a better way to think about culture is to examine the different "levels" at which culture exists. All organizations' corporate culture includes three levels (Schein, 1999), which are described below.

Level One: Artifacts.

Artifacts are defined as what can be observed, seen, heard, and felt, in an organization. Artifacts include visible organizational structures and processes. Culture is considered to be clearly visible at this level and has an immediate emotional influence, which could be positive or negative, on the observer (Schein, 1999, pp. 15-16).

Level Two: Espoused Values.

Schein (1999, p. 17) points out that an organization's espoused values are the "reasons" an organizational insider would give for the observed artifacts. Espoused values generally consist of the organization's official viewpoints, such as mission or vision statements, strategy documents, and any other documents that describe the organization's values, principles, policies, ethics, and visions. Schlienger and Teufel (2002) believe that the espoused values are partially visible in the organization and reflect the values of a particular group of individuals.

Level Three: Shared Tacit Assumptions.

Schein, (1999, p. 19) states that organizations must develop shared tacit assumptions to ensure their success. Shared tactic assumptions are formed in the early years of the organizations. Basic tacit assumptions are the heart of the corporate culture as they represent the commonly learned values and assumptions of employees. Basic tacit assumptions are hidden and largely unconscious, and occur very much at the individual level.

Conceptual Framework Development

This paper has presented ISM factors and culture factors that aid or hinder the implementation and the adoption of IS culture and practices in developing countries. Figure 1 represents the themes and factors that were found in the literature analysis to be implicated in the adoption of IS culture and practices.

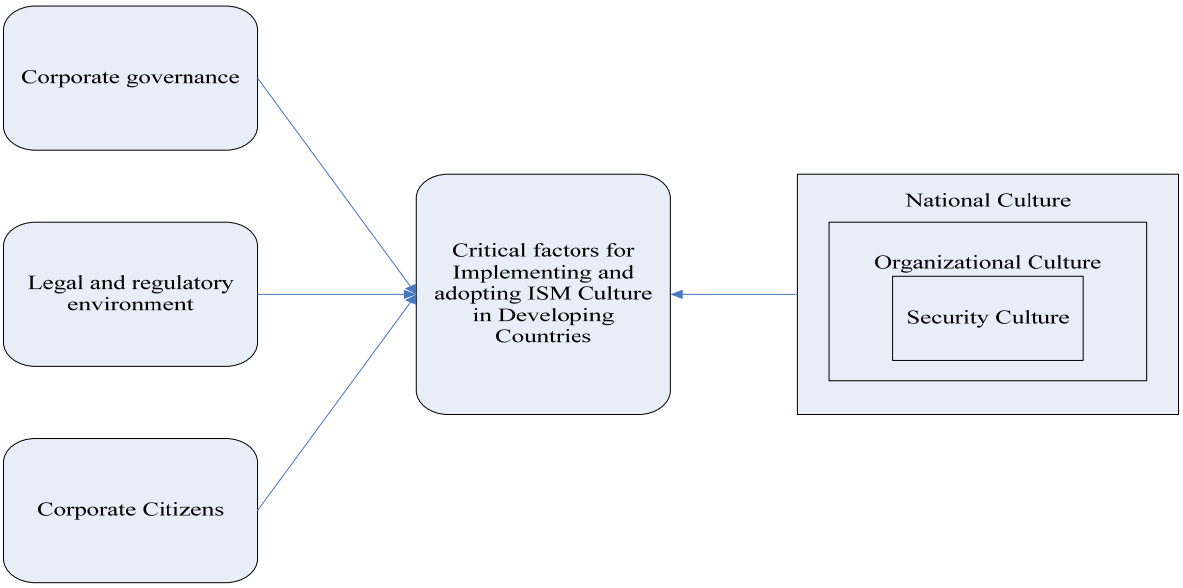

Figure 1 Factors for implementing and adopting IS culture and practices in Saudi Arabia

CONCLUSION AND FUTURE WORK

This paper has highlighted the important of ISM factors and cultural factors in Saudi Arabia that have not been widely addressed in the discipline specific or related literature. This study believes that there is a gap in terms of addressing the influences of both ISM factors and cultural factors on the adoption of security culture in any organization. ISM factors were incorporate into three themes such as corporate citizenship that include information security awareness and training programs, legal and regulatory environment that include ISM standardization and best practices and information security policy, and corporate governance that include top management support for ISM, information security compliance and information security risk analysis. In addition, a cultural theme that include national and organizational culture that has a strong influence on the adoption of security culture. Therefore, we aim to addresses the gap in knowledge about ISM factors and cultural factors that will lead to the implementation and the adoption process of IS cultural and practices in Saudi Arabia. We plan to test the conceptual framework explicated in figure 1 which results from our literature analysis in a large-scale project consisting of a quantitative survey and in-depth interviews to examine the influence of the factors identified and their impact on adopting IS culture and practices in Saudi Arabia.

We will investigate this conceptual framework on a range of different sized Saudi Arabia organizations and various types of organizations (government, semi-government, and private) and industries (financial, healthcare, IT, manufacturing, construction, educational, insurance). Multiple participants within each organization will be asked to respond to the survey and participate in the interviews including top management, operation managers, IS managers and officers or any member of the organization representing the security department, IT managers, and staff, and technical, and general staff.

ACKNOWLEDGEMENTS

The authors would like to thank Professor von Solms, S. H. from University of Johannesburg for his valuable discussions in this study.

REFERENCES

Albert, C., & Dorofee, A. (2003). *Managing Information Security Risks, the OCTAVE Approach*. New York, USA: Addision-Wesley.

Atkinson, P. (1997). *Creating culture change – strategies for success*. Bedfordshire, England: Rushmere Wynne.

BACKGROUND NOTE: SAUDI ARABIA (2009). *Bureau of Near Eastern Affairs, US department of state.* Retrieved 10 June 2009, from http://www.state.gov/r/pa/ei/bgn/3584.htm

British Standards Institute. (1995). *BS7799: Part 1, Information Security Management: Code of Practice for Information Security Management Systems*. London: BSI.

British Standards Institute. (1999). *Information Security Management-BS 7799-1:1999*. London: BSI.

Beach, L. R. (1993). *Making the right decision. Organizational culture, vision and planning*. Eaglewood Cliffs, New Jersey: Prentice Hall.

Beautement, A., Sasse, M., A., and Wonham, W. (2008). *The Compliance Budget: Managing Security Behavior in Organizations.* Paper presented at the Workshop on New Security Paradigms, Olympic, California, USA.

Bjerke, B., & Al-Meer, A. (1993). Culture's consequences: management in Saudi Arabia. *Leadership & Organization Development Journal, 14*(2), 30-35.

Caelli, W., Longley D., & Shain, M. (1989). *Information Security for Managers*. UK: Stockton Press.

Ceraolo, J. P. (1996). Penetration testing through social engineering. *Information Systems Security, 4*(4), Winter.

Chadhar, M., A. & Rahmati, N. (2004). *Impact of national culture on ERP systems success.* Paper presented at the Second Australian Undergraduate Students' Computing Conference, Melbourne, Australia.

Chang, S., E., Lin, C. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems, 107*(3), 438-458.

Chen, C., C., Medlin, D., B. and Shaw, R., S. (2008). A cross-cultural investigation of situational information security awareness programs. *Information Management & Computer Security, 16*(4), pp. 360-376.

Chia, P., Maynard, S., and Ruighaver, A.,B. (2002). *Exploring Organizational Security Culture: developing a comprehensive research model.* Paper presented at the IS ONE World Conference, Las Vegas, Nevada USA.

da Veiga, A., Martins, N., & Eloff, J.H.P. (2007). Information security culture – validation of an assessment instrument. *Southern African Business Review, 11*(1), 147-166.

Deal, T., E. and Kennedy, A. A. (1982). *Organization cultures: the rites and rituals of organization life*. Reading, UK: Addison-Wesley.

Deloitte, T., Tohmatsu. (2005). Global security survey.

Dhillon, G. (1999). Managing and controlling computer misuse. Information Management & Computer Security, 7(4), 171-175.

Eloff, J., & Eloff, M. (2003). ISM system components and investigating the protection for these components. *South African Institute of Computer Scientists and Information Technologists*, 130-136.

Eloff, M., M., and von Solms, S., H. (2000). Information Security management: A Hierarchical Approach for various frameworks. *Computer & Security, 19*(3), 243-256.

Energy Information Administration. (2009). Retrieved September 5th, 2009 from http://tonto.eia.doe.gov/country/index.cfm?view=reserves

Ernst and Young (2001). *Information Security Survey. London, Ernst & Young*

Ernst & Young. (2002). *Global Information Security Survey. London: Ernst & Young*

Finestone, N., & Snyman, R (2005). Corporate South Africa: making multicultural knowledge sharing work. *Journal of Knowledge Management, 9*(3), 128-141.

Finne, T. (1998). A Conceptual Framework for Information Security Management. *Computers & Security, 17*, 303-307.

Fourie, L., C., H. (2003). The management of Information Security- A South Africa case study. *South Africa Journal of Business Management 34*(2), 19-29.

Fulford, H., Doherty N., F. (2003). The application of information security policies in large UK-based organizations: an exploratory investigation. *Information Management & Computer Security, 11*(3), 106-114.

Garg, A., Curtis, J. and Halper, H. (2004). "Quantifying the financial impact of IT security breaches". *Information Management & Computer Security, 11*(2), 74-83.

Gerber, G., von Solms, R., & Overbeek, P. (2001). Formalizing information security requirements. *Information Management & Computer Security, 9*(1), 32-37.

Gerber, M., and von Solms, R. (2005). Management of risk in the information age. *Computers & Security 24*, 16-30.

Hagberg Consulting Group. (1999). *Corporate culture/organizational culture: understanding and assessment*.

Higgins, H. N. (1999). Corporate system security: towards an integrated management approach. *Information Management & Computer Security, 7*(5), 217-222.

Hill, C., Loch, K, Straub D., W. and El-sheshai, K. (1998). A Qualitative Assessment of Arab Culture and Information Technology Transfer. *Journal of Global Information Management, 6*(3), 29-38.

Hinde, S. (2002). Security survey spring crop. *Computer & Security, 21*(4), 310-321.

Hofstede, G. (1984). *Culture's Consequences: International Differences in Work Related Values*. Beverly Hills: Sage Publications.

Hofstede, G. (1997). *Culture and Organizations: Software of the Mind*. New York, NY: McGraw-Hill.

Hofstede, G. (2001). *Culture's Consequences: Comparing Values, Behaviors, Institutions, and Organizations Across Nations*. Thousand Oaks, Calif: Sage Publications.

Höne, K., Eloff, J., H., P. (2002). Information security policy — what do international information security standards say?. *Computers & Security, 21*(5), 402-409.

Hong, K., Chi, Y., Chao, L., & R., Tang, J. (2006). An empirical study of information policy on information security elevation in Taiwan. *Industrial Management & Data Systems, 106*(3), 345-361.

Hong, K., Chi, Y., Chao, L., R., Tang, J. (2003). An integrated system theory of information security management *Information Management & Computer Security, 11*(5), 243-248.

How to 27000 Works. (2009). Retrieved April 5, 2009, from http://www.gammassl.co.uk/bs7799/works.html

Idris, A. M. (2007). Cultural Barriers to Improved Organizational Performance in Saudi Arabia. *SAM Advanced Management Journal, 72*, 36-53.

Information System Audit and Control Association. (2009). Retrieved June 5, 2009, from http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders1/COBIT6/Obtain_COBIT/CobiT4.1_Brochure.pdf

Karabacak, B., and Sogukpinar, I. (2006) A quantitative method for ISO 17799 gap analysis. *Computers & Security, 25*(2), 413-419.

King Committee on Corporate Governance. King II Report. (2002). South Africa: Institute of Directors (IOD).

Knapp, K. J., Marshall, T.E., Rainer, R.K. and Morrow, D.W. (2004). *Top Ranked Information Security Issues*. Paper presented at the 2004 International Information Systems Security Certification Consortium (ISC) 2 Survey Results.

Knapp, K. J., Marshall, T.E., Rainer, R.K. & Morrow, D.W. (2007). Do Information Security Professionals and Business Managers View Information Security Issues Differently? . *Information System Security, 16*, 100-108.

Kowk, L., Longley, D. (1999). Information security management and modeling. *Information Management & Computer Security, 7*(1), 30-39.

Loch, K., D, Straub, D., W, 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), 46-63.

Luthy, D., & Forcht, K. (2006). Laws regulations affecting information management and frameworks for assessing compliance. *Industrial Management & computer Security, 14*(2), 155-166.

Ministry of planning, (2009). The Long Term Strategy of the Saudi Economy. Retrieved 14 May2009, from http://www.mep.gov.sa/index.jsp;jsessionid=7B955F78E47998F5AF703B7D276902CB.beta?event=ArticleView&Article.ObjectID=53

Ministry of Communications and Information Technology. (2006). *the National Communications and Information Technology Plan. The Vision towards the Information Society* Retrieved 10 June 2009, from http://www.mcit.gov.sa/NR/rdonlyres/E8C255A7-E423-4F36-B9B3-C5CAAB6AE87A/0/2NICTPEng.pdf?

Mitchell, R., C., Marcella, R., and Baxter, G. (1999). Corporate information security management. *New Library World, 100*(1150), 213-227.

Nosworthy, J. D. (2000). Implementing Information Security In The 21st Century – Do You Have the Balancing Factors? *Computers & Security, 19*, 337 – 347.

Pfleeger, C. P. (1997). *Security in Computing* (2nd ed.). Englewood Cliffs, NJ: Prentice Hall International.

Rathmell, A. (2001). Protecting critical information infrastructures. *Computers and Security, 20*, 43-52.

Ruighaver, A., B., Maynard, S., B. and Chang, S. (2007). Organizational security culture: Extending the end-user perspective. *Computers & Security, 26*(1), 56-62.

Saleh, M., S., Alrabiah, A., Bakry S., H. (2007). A STOPE model for the investigation of compliance with ISO 17799-2005. *Information Management & Computer Security, 15*(4), 283-294.

Saudi Arabian General Investment Authority (SAGIA) (2009). Retrieved 18 June 2009, from http://sagia.gov.sa/english/index.php?page=introduction

Schein, E., H. (1999). *The Corporate Culture Survival Guide*. San Francisco: Jossey-Bass.

Schlienger, T., and Teufel, S. (2002). *Information Security Culture: The Socio-Cultural Dimension in Information Security Management*. Paper presented at the Security in the Information Society: Visions and Perspectives.

Schlienger, T., and Teufel, S. (2003). *Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture.* Paper presented at the DEXA Workshops.

Schultz, E. (2004). Security training and awareness—fitting a square peg in a round hole. *Computers & Security, 23*(1), 1-2.

Security Awareness Index Survey. (2002). Retrieved June 15, 2009, from http://www.netiq.com/news/releases/release.asp?cid=20021213144711QDNH

Senge, P. M. (1990). *The Fifth Discipline: The Art and Practice of the Learning Organization*. New York, USA: Doubleday Currency.

Sengun, Y., and Janell, D., T. (2003). Does culture explain acceptance of new products in a country? An empirical investigation. *International Marketing Review, 20*, 377.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 18*(1), 31-41.

Smith, S., Jamieson, R., and Winchester, D. (2007). *An Action Research Program to Improve Information Systems Security Compliance across Government Agencies.* Paper presented at the 40th Hawaii International Conference on Systems Science (HICSS), Hawaii, USA.

Straub, D. W. (1990). Effective IS security: an empirical study. *Information System Research, 1*(2), 255-277.

Straub, D. W., and Welke, R.J. (1998). Coping with systems risk: security planning models for management decision making. *MIS Quarterly, 22*(4), 441-464.

Thomson, K., von Solms, R., and Louw, L. (2006). Cultivating an organizational information security culture. *Computers & Security 10*, 7-11.

Thomson, M., E. & von Sloms, R. (1998). Information Security awareness: educating your users effectively. *Information Management & Computer Security, 6*(4), 167-173.

Tsiakis, T., and Stephanides, G. (2005). The economic approach of information security. *Computers & Security, 24*(2), 105-108.

Turban, E., Mclean, E., & Wetherbe, J. (1996). *Information Technology For Management: improving Quality and Productivity.* USA: John Wiley & Sons Inc.

USSABC. (2008). The Saudi Arabian Economy Retrieved June 16, 2009, from http://www.us-sabc.org/i4a/pages/index.cfm?pageid=3367

van Niekerk, J., and von Solms, R. (2005). *A holistic framework for the fostering of an information security sub-culture in organizations.* Paper presented at the 4th Annual ISSA Conference South Africa.

Voelpel, S., C, & Han, Z (2005). Managing knowledge sharing in China: the case of Siemens Share Net. *Journal of Knowledge Management, 9*(3), 51-63.

von Solms, R. (1996). Information Security Management: The Second Generation. *Computer & Security, 15*, 281-288.

von Solms, R. (1999). Information security management: why standards are important. *7, 1*(50-57).

von Solms, R., & von Solms, S.H. (2004). From policies to culture. *Computer & Security, 23*, 275-279.

von Solms, S. H. (2005). Information Security Governance- Compliance management vs. operational management. *Computers & Security, 24*, 443-447.

von Solms, S. H. (2000). Information Security- The Third Wave?. *Computer & Security, 19*, 615-620.

von Solms, S. H. (2001). Corporate Governance and Information Security. *Computers and Security, 20*, 215 – 218.

von Solms, S. H., & von Solms, R. (2004). The 10 deadly sins of Information Security Management. *Computer & Security, 23*, 371-376.

Vroom, C., and von Solms, R. (2004). Towards information security behavioral compliance *Computers & Security, 23*, 191-198.

World Bank. (2009). Retrieved June 15, 2009, from http://web.worldbank.org/WBSITE/EXTERNAL/DATASTATISTICS/0,,contentMDK:20420458~menuPK:64133156~pagePK:64133150~piPK:64133175~theSitePK:239419,00.html

Zakaria, O., Jarupunphol, P., and Gani, A. (2003). *Paradigm Mapping for Information Security Culture Approach.* Paper presented at the 4th Australian Information Warfare and IT Security Conference Adelaide, Australia.

COPYRIGHT