The Role and Impact of Cultural Dimensions on Information Systems Security in Saudi Arabia National Health Service

Saleh Alumaran, Giampaolo Bella and Feng Chen
Software Technology Research Laboratory
Department of Computer Science and Informatics
De Montfort University, Leicester, UK

ABSTRACT

Organisation culture has become an important part of an organisation's strategy to promote its performance and productivity. The study of organisation culture's role on information security has attracted scholars as well as industry leaders to research the topic and find appropriate tools and approaches to develop positive information about security culture. Information security is one of the main concerns of organisation management and has become one of the information management strategies. Healthcare service providers manage, control and transmit large amounts of information in traditional, hardcopy, and electronic records and health service information security has become one of the main challenges of the health services authorities worldwide. Health services in Saudi Arabia have expanded in the last few decades, and the implementation of information security systems has become an essential part of health services. However, the health services lack any framework for the information security culture that the healthcare authority can use and adopt. This study is the first research in the field measuring the role and impact of culture on information management in Saudi Arabia. The research investigated and analysed the role and impact of cultural dimensions on information security in Saudi Arabia health service. Hypotheses were tested and two surveys were carried out in order to collect data and information from three major hospitals in Saudi Arabia (SA). The first survey identified the main cultural-dimension problems in SA health services and developed an initial information security culture framework model. The second survey evaluated and tested the developed framework model to test its usefulness, reliability and applicability. The framework can be used as part of the authority's strategic planning on information security policies, employees' training and the structure and activities of health services.

General Terms

Security, Health Information Management, Culture, Culture Dimension.

Keywords

Culture Dimension, Information Security, Electronic Health Records, Information Management

1. INTRODUCTION

Health services information has seen sharp changes in the last few decades due to changes in the health services operations and patients' and staff members' rights towards their personal information, and has also shifted from traditional handling and accessing of patients and staff information to the effective use of electronic technology. These have led to an understanding of the importance and the needs for effective policy and strategy to ensure health services information security. Effective information security also helps in improving and promoting health services [1].

Cultural dimensions have become an important part of an organisation's strategy to promote its performance and productivity. The study of organisations attracted scholars as well as health services industry to research the topic and find appropriate tools and approaches to develop a positive culture. There is a large number of studies on role of culture dimensions on society and an organisation. Reference [2] argued that organisations need to change to the holistic management of information security to establish an effective information security culture. The vast majority of studies regarding Saudi national health services are on the use of technology to protect and secure health services information. On the other hand, there is a lack of research on the role and impact of organisations' cultural dimensions on information security. Reference [3] argued that information security needs to be focused on the organisation's behaviour. They stressed that the organisation's success or failure depends on the employees' behaviour within the organisation. They indicated that an information security-aware culture will minimise risks to information assets and specifically reduce rates of employee misbehaviour.

Saudi Arabia is in the process of developing its institutions and healthcare system to cope with the socio-economic changes of the Kingdom as well as regional and internal changes. The main challenges in the Kingdom's development processes are in using technology in management.

One of the main challenges of the introduction and implementation of technology is the cultural change that will occur as a result. Cultural change can be found in the organisational and national levels. The Kingdom has no problem in investing in technology, hardware and software due to the large revenue that it receives from oil. The challenge of the Kingdom is in investing such revenue in developing its institutions such as the healthcare services.

Information can be protected by two strategies. The first is the use of technology to protect valuable information, which is required when intruders try to access and transfer information. The second is the human element, wherein the user can either deliberately or accidentally abuse the information by passing information to a third party without consent of the information owners. This research is focusing on the role of the human element of the health services culture on information security. The study of organisations' information security cultures has attracted scholars as well as healthcare services industry to research the topic and find appropriate tools and approaches to develop a positive culture. The vast majority of studies in

Saudi national health services are on the use of technology to protect and secure health services information. On the other hand, there is a lack of research on the role and impact of an organisation's cultural dimensions on information security. This research investigated and analysed the role and impact of cultural dimensions on information security in Saudi Arabia health service.

2. PREVIOUS WORK

One of the most well-established and recognised study of cultural dimensions in the literature is Hofstede's dimensions of culture. The dimensions are based on comprehensive research carried out on 72 countries between 1967-1973. The research was based on a designed questionnaire that aimed to identify the dimensions of organisation culture. The research collected a total of 166,000 questionnaires from the surveyed countries [4]. The questionnaire responses were analysed based on theoretical reasoning and statistical analysis to explain the differences between the surveyed countries' cultures. The author identified, based on the survey, four main cultural dimensions: power distance, uncertainty avoidance, individualism and collectivism, as well as on masculinity and femininity [5]. A fifth dimension added to the four dimensions is based on a survey of Chinese national culture, Long-term vs. Short term Orientation Dimension [5].

2.1 Power Distance (PD) Dimension

This dimension is based on the suggestion that people in the society are unequal in status and social power. Hofstede argued that power is distributed unfairly in any society. This creates a distance or gap in the power within the society. Power distance can be defined as "a measure of the interpersonal power between boss (B) and subordinate (S)" [4]. The power distance in the society was also explored and can be defined as: "the degree of inequality in power between a less powerful Individual (I) and a more powerful other (O), in which (I) and O belong to the same (loosely or tightly knit) social system".

One of the concerns of Hofstede's dimensions is the gender power within the society. This argument is based on the existence of the power distance between male and female power within one society. This may depend on the society's national culture. Stedham [6] argued that Hofstede's dimensions are gender-specific, with only one exception: masculinity/feminity. The author also argued that gender power distance exists in Japanese society. This needs to be considered when analysing Japanese culture. The gender power distance dimension can be critical in a male-dominant society, in which the power rests mainly in the hands of the male. In such a society, females have less power in the society and are controlled by males. From the Saudi Arabian point of view, the gender power distance may need to be considered in order to identify and establish the role and impact of the males' power as being dominant on the society's social and cultural behaviour and in the decision-making process.

2.2 Uncertainty Avoidance (UA) Dimension

This dimension focuses on the level of stress in the society in the face of unknown and unexpected future events. This represents society's ability and willingness to embrace change and reluctance to cope and deal with ambiguity. From the organisation's point of view, the organisation culture can be influenced by unpredicted future events, such as sudden periods of recession or war.

2.3 Individualism vs. Collectivism Dimension

This dimension is distinguished between individual and group behaviour within the society. Hofstede [4] described this dimension by stating that it is "the relationship between the individual and the collective that prevails in a given society". Individualism describes when people place their personal interests and goals ahead of those of the social group within the society. It is emphasised that how the individual behaves within the society is based on his or her own interest and goals, regardless of the group's interest and goals. Hofstede [4] argued that the type of society, particularly whether it is organised from the point of view of individualism or collectivism, has an impact on the organisation's employees' reasons to comply with an organisation's policy and requirements. There are several factors of individualism behaviour within an organisation. These factors include social norms, levels of education, organisation culture and organisation history [4]. One of the key issues explored from the individualism and collectivism perspectives is the role and impact of societal norms on the individual's relationship with the organisation. The norm prevalent in a given society as to the degree of individualism/collectivism expected from its members will strongly affect the nature of the relationship between a person and the organization to which he or she belongs [5].

One of the distinctions between individualism and collectivism is that individuals from cultures that adhere to collectivism show a greater tendency to cooperate in the organisation and society at large. They feel more towards people within their cultural group, and they feel more part of the group. On the other hand, individualists represent autonomous entities that are independent of their cultural group. Individualists tend to be more competitive in the work place when compared with collectivists, and they try to improve themselves due to their own personal interests.

2.4 Masculinity vs. Femininity (MF) Dimension

This dimension can be argued as the only dimension that recognises the differences between males' and females' roles in a society. Seldham, [6] described this dimensions as "the degree to which gender roles are clearly differentiated within a country. In masculine countries, gender roles are very distinct and separated. Men are assertive and tough; women are modest and tender".

This dimension argued that males score significantly higher than the females, regarding their differences in emotional actions [6].

2.5 Long-term vs. Short term Orientation Dimension

This dimension was added to the original Hofstede dimensions based on a Chinese survey, the Chinese Value Survey (CVS) around the mid 1980s. This dimension is considered to be the fifth dimension of culture and is used to analyse and discuss cultural issues. The dimension is based on the teachings of Confucius, particularly on both of its poles' items. The dimension argues in opposing short-term aspect of the Confucian thinking and thrift and focuses on personal stability, respect and valuing traditions. In simple term, individuals value his or her historical tradition and values [4].

3. INFORMATION SECURITY (IS) CULTURE

Humans play a major role in managing and controlling healthcare services information besides the use of technology. Extensive research and development have been achieved in the last few decades in using technology to protect healthcare information through strictly controlling access to the information by using technology such as specific usernames and passwords. Technology also helps with dividing information and users into groups based on their jobs' roles and responsibilities, and this will help protect information. Another concern in healthcare information is the role of humans in healthcare service information security. However, the role of humans in information handling is consistently referred to as the weakest link in information security [7]. Schulz [8] argued that information security is not a technical problem or issue that needs to be considered but that it is also a problem that concerns people, and this needs to be considered carefully by information management authority members.

One of the issues raised in the literature regarding the role of people entails the users' awareness and understanding of what being 'secure' actually means [9]. This may be due to the lack of training and educational programmes regarding information security. Chan et al. [10] indicated that one of the main causes of concern and challenges in an organisation is that its employees often fall short in complying with information security policies and guidelines. It is important to stress that maintaining an organisation's information security is not only the responsibility and duty of the information technology specialist within the organisation, but it is also the duty and responsibility of all of the employees within the working environment of the organisation [11]. The author argued that information users need to be aware of their exact roles and responsibilities in protecting the information and that they should respond by taking appropriate actions and measures when dealing with any potential security issue.

Several authors stressed clearly that an organisation's information security problems are evidently linked to its employees' behaviour [12][13][14]. Technical controls can provide substantial protection against many of these threats, but they alone do not provide a comprehensive solution [11]. These technological methods of protecting information may be effective in their respective ways; however, many losses are not caused by a lack of technology or faulty technology but, rather, by users of technology and faulty human behaviour [11].

3.1 Leadership and Organization Culture

An organisation's employees rely on the established system to carry on their job. They provide little resistance and stress towards such a system in an attempt to ensure their job security and avoid any conflicts with the management [15]. From the health services employees' points of view, nursing practices have a strong history of being task-focused due to the nature of the job activities [16]. Ruighaver et al. [17] explained that within an organisation, information security is primarily a management problem, and how management deals with information security is a direct reflection of an organisation's culture. One of the organisation culture's frameworks is the basis of truth and rationality. The basis of truth and rationality is the first component of the organisational culture framework, and it refers to the truth in security beliefs and actions.

3.2 Current Drives for IS Culture Policy

This research reveals several drives for SA national health services authority to introduce and implement clear strategies to promote IS culture in the services. One of the drives is the current understanding and awareness of Saudi patients and employees as regards their rights towards their personal information [18]. Therefore, the working environment culture needs to be promoted to protect the individual's right towards their information through the demonstration of appropriate behaviour by employees. Currently, there is a clear IS culture policy in this direction. Therefore, the authority needs to implement an action plan through developing a clear strategy in this direction.

The second drive is to avoid any legal conflict due to the expansion and effectiveness of legal firms in supporting patients' claims. This has become an important drive due to the fact that a large number of non-Saudi employees and companies operate in Saudi Arabia. The other important factor is the image of the service, which needs to be high on the agenda of the authority, due to the support and investment of the authority in the service. Any issue harming the image of the service may induce prejudice on the service's authority image and commitment towards providing appropriate healthcare services.

It also has been observed and explored in several interviews that employees leave their computer or monitor on, while they go for a short break leaving their desks. This leaves the information and access to the information system to be exposed by any intruder. The other practice identified as norms amongst some of the employees includes providing their password to their colleagues. Some hospitals are in the process of introducing and implementing electronic recording and transmission of patient records as part of the hospital's operations, which they are implementing to improve the hospital's efficiency as well as the healthcare system. However, from the information security culture point of view is a challenge. This requires a change in the employees' behaviour towards information security. The employees need awareness, knowledge and understanding of the electronic process to ensure that information cannot be transmitted and/or accessed by non-authorised persons.

4. INFORMATION SECURITY CULTURE AND SUB-CULTURE DIMENSIONS

National Culture Dimension: One of the dimensions identified in the data analysis is the Saudi national culture. The analyses showed that the national culture plays a role on the staff behaviour, such as behaviour towards information security. The national culture has three main sub-cultural dimensions. These sub-cultural dimensions are the working values and norms, tribe values and norms and attitudes and perceptions towards women.

SA Health Services Leadership: Establishing an effective information security culture requires appropriate health services leadership. Leadership has been identified as one of the dimensions that contribute towards the staff members' attitudes, which in turn contributes to the hospital culture. The leadership has sub-cultural dimensions, such as power sharing, leading by example and developing a vision towards information security within the hospital culture.

Employees' Trust: Trust amongst employees has been identified as one of the dimensions that needs to be considered in the hospital's culture of information security. The trust can be developed and enhanced by social Interaction, respect and understanding. Trust amongst the employees as well as between the employees and senior management contributes to the hospital information security culture.

Technology Dimension: The hospital's use of technology in its activities and communication contributes to the hospital's culture. The technology dimension contains an Intranet and communication system sub-culture. The Intranet can help in promoting and enhancing information security, training and updating staff with organisation new policy, procedures and management operations. On the other hand, technology has become an integral component of communication amongst the hospital medical and non-medical staff members. Communication helps in building staff members' understanding and awareness, and these help in developing trust amongst the employees and the employers.

Multicultural Interaction: The employees' multicultural background interaction dimensions has sub-cultural dimensions such as language, working values and norms and national culture.

Job Role: An individual's job role within the hospital working environment has an impact on the individual's behaviour towards information security. The job role has sub-cultural dimensions including job security and motivation (or job satisfaction).

Developing and Implementing Information Security Policy: Once the hospital develops an awareness and understanding of the main drives for its staff members' behaviour, the hospital authority can then develop and implement effective employees' behaviour expectations towards information security.

Promoting Information Security Culture: Understanding and awareness of the employees' behaviour towards information security can help in promoting and enhancing the hospital culture. From this research perspective, understanding and analysing staff behaviour will help in recommending practical steps for promoting and enhancing a positive hospital information security culture.

5. RESEARCH HYPOTHESES

The research developed information security culture model to help identify main cultural dimensions that are influencing individual's behaviour towards information security. This achieved by testing several hypotheses related to these dimensions. These hypotheses are:

Hypothesis 1: H1: Organisational leadership is positively related to the employees' attitude towards health information security.

Hypothesis 2: H2: Employees' job satisfaction and job security are positively related to the employees' attitudes towards information security.

Hypothesis 3: H3: Trust is positively related to the employees' attitudes towards information security.

Hypothesis 4: H4: Organisations information security policies are positively related to the employees' attitudes towards information security.

Hypothesis 5: H5: Organisations' communication is positively related to the employees' attitudes towards information security.

Hypothesis 6: H6: Employees' intentions towards information security are positively related to the employees' attitudes toward information security.

Hypothesis 7: H7: Employees' intentions and their actual behaviour are positively related to information security.

6. RESEARCH METHOD

The research adopts a mixed method multiple methods approach in collecting data. This includes collecting quantitative and qualitative data to support outcomes analysis. This type of approach helps in providing data and information from different resources to achieve the research's aims and objectives as well as in answering the research main questions. The mixed approach used in this research includes collecting qualitative and quantitative data. Data from the research fieldwork namely, Saudi Arabian health services, is needed to provide raw data that can be used to identify and explore the current information security culture in the service and to explore the main challenges in promoting and enhancing information security culture. The data collection involved distributing a semi-structured questionnaire to three main hospitals in Saudi Arabia and conducting in-depth face-to-face interviews with key personnel of the three hospitals to explore hospital key personnel members' opinions and attitudes towards information security culture as well as the main factors influencing their information security culture. The main purposes of the interviews are to explore and identify information security culture to help with developing the initial information security culture model. The main outcomes of this stage with the use of outcomes of the literature review helped in developing the information security culture model.

6.1 Modelling and Evaluation

Developing an information security culture model is one of the main objectives of this research. The purpose of the model is to provide the SA health authority figures with a model that helps in developing and enhancing their information security culture strategy and policy. The model has been developed based on two main outcomes. The first outcome entails the main findings of the data analysis of the first survey on the SA health services, and the second includes the main findings of the literature survey.

The model has been developed and designed based on a set of cultural dimensions identified and explored by the survey data analysis and the literature survey. It consists of cultural dimensions and sub-dimensions that influence the health services' information security cultures and the employees' attitudes towards information security behaviour. The model relates and identifies the role of the cultural dimensions and the sub-dimensions to the hospital culture and the behaviour of the staff towards information security culture. The information security culture helps in developing the information security culture policy.

There is a need for a clear and effective hospital policy to establish and clarify the expected interactions and behaviours towards information security. The SA health authority is in need of a framework model for developing an effective information security culture policy to protect the dignity of the patient's medical records. The policy model is based on the main outcomes of the first model- namely, the information security model. The policy takes in consideration the cultural dimensions and the staff members' attitudes and behaviours towards the information security model.

The developed model was evaluated to ensure its applicability, usefulness and practicality to SA health authority members. The evaluation of the model is based on a second survey on the research fieldwork namely, regarding the Saudi Arabian health services. The second survey is based on collecting quantitative and qualitative data by using the same survey that the hospitals used to evaluate the developed models.

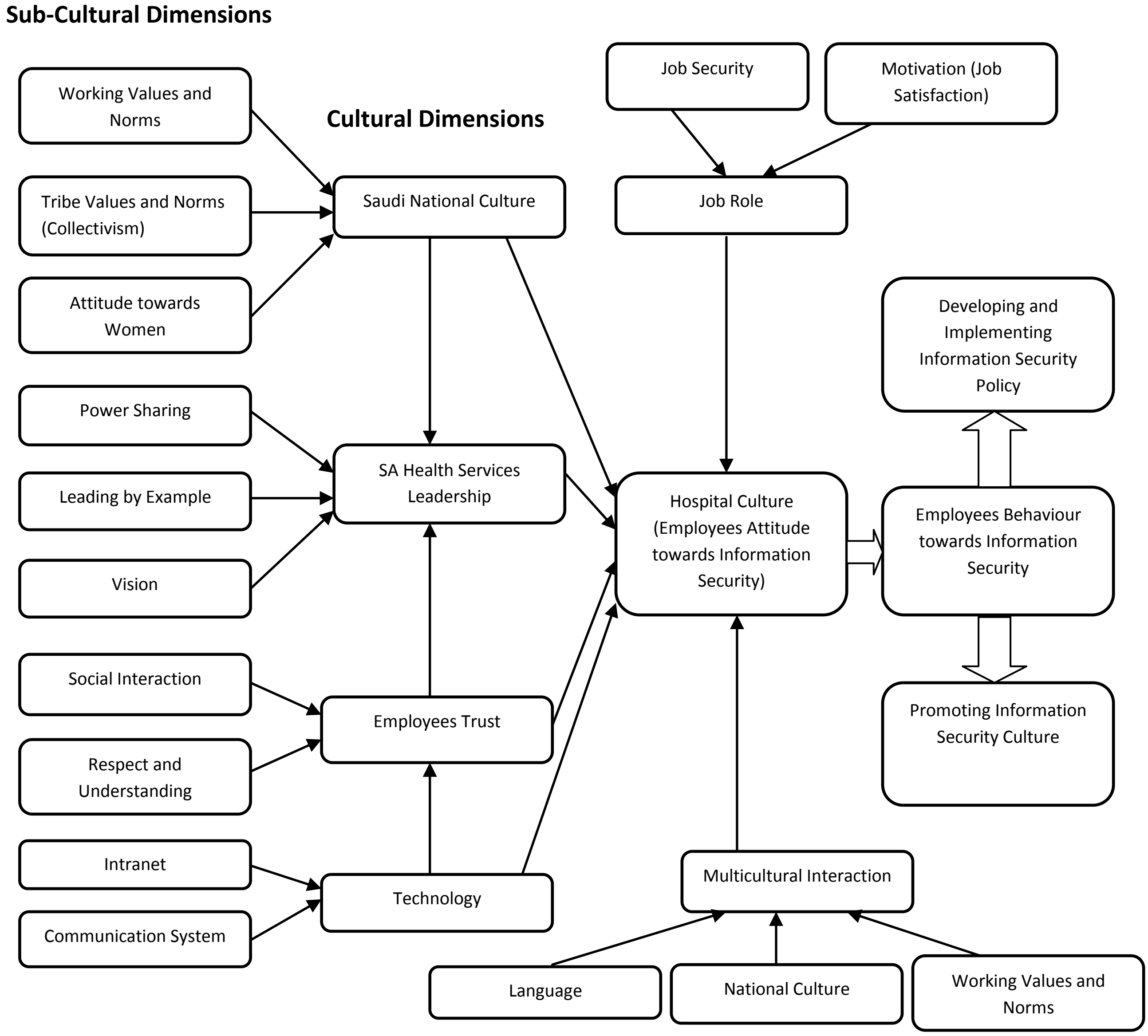
Sub-Cultural Dimensions
Cultural Dimensions
Working Values and Norms
Tribe Values and Norms (Collectivism)
Attitude towards Women
Saudi National Culture
Power Sharing
Leading by Example
Vision
SA Health Services Leadership
Social Interaction
Respect and Understanding
Employees Trust
Intranet
Communication System
Technology
Job Security
Motivation (Job Satisfaction)
Job Role
Hospital Culture (Employees Attitude towards Information Security)
Developing and Implementing Information Security Policy
Employees Behaviour towards Information Security
Promoting Information Security Culture
Multicultural Interaction
Language
National Culture
Working Values and Norms

Figure 1: Model of the Study

7. RESULTS

A total of 800 questionnaires were distributed to three main hospitals in Saudi Arabia. The number of valid and completed responses that we received was 588.

For the statement: 'Hospital leadership creates an information security environment where the employee takes ownership of his or her tasks'. The vast majority, 367 out of 588, strongly agreed or agreed with the statement, and only 138 out of 558 strongly disagreed or disagreed.

For the statement: 'Hospital asks employees for their vision of where they see information security going and then uses their vision where appropriate'. The vast majority, 424 out of 588, strongly agreed or agreed with the statement, and only 88 out of 558 strongly disagreed or disagreed.

For the statement: 'Hospital leadership likes to share information security power with employees'. The vast majority, 337 out of 588, strongly agreed or agreed with the statement, and only 146 out of 558 strongly disagreed or disagreed.

For the statement: 'Hospital takes group vote on what to do next regarding the hospital information security policy'. The vast majority, 308 out of 588, strongly agreed or agreed with the statement, and only 161 out of 558 strongly disagreed or disagreed.

For the statement: 'National culture has influenced the leadership style in the hospital information security culture'. The vast majority, 444 out of 588, strongly agreed or agreed with the statement, and only 82 out of 558 strongly disagreed or disagreed.

For the statement: 'National culture values and norms have a role in the leadership information security decision-making process'. The vast majority, 372 out of 588, strongly agreed or agreed with the statement, and only 138 out of 558 strongly disagreed or disagreed, as shown in figure 2.

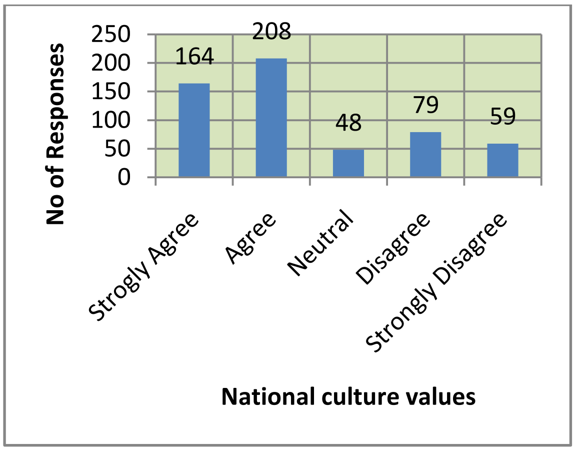

Figure 2: National culture values and norms have a role in the leadership IS decision-making process

For the statement: 'Change in the hospital information security policy from traditional to electronic is a challenge'. The vast majority, 321 out of 588, strongly agreed or agreed with the statement, and only 159 out of 558 strongly disagreed or disagreed.

For the statement: 'The hospital uses an effective information security policy to protect electronic patient records'. The vast majority, 332 out of 588, strongly disagreed or disagreed with the statement, and only 134 out of 558 strongly agreed or agreed, shown in figure 3.

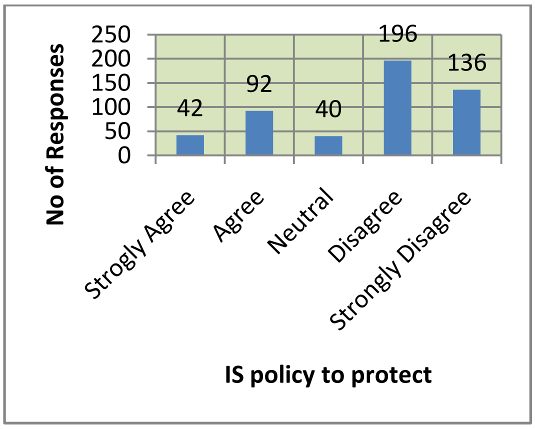

Figure 3: The hospital uses an effective IS policy to protect EPR

For the statement: 'Hospital employees have positive norms and values towards information security'. The vast majority, 331 out of 588, strongly disagreed or disagreed with the statement, and only 151 out of 558 strongly agreed or agreed.

For the statement: 'Hospital has a clear information security policy'. The vast majority, 416 out of 588, strongly disagreed or disagreed with the statement, and only 108 out of 558 strongly agreed or agreed.

For the statement: 'Trust among the hospital employees is important for hospital information security'. The vast majority, 328 out of 588, strongly disagreed or disagreed with the statement, and only 163 out of 558 strongly greed or agreed, as seen in figure 4.

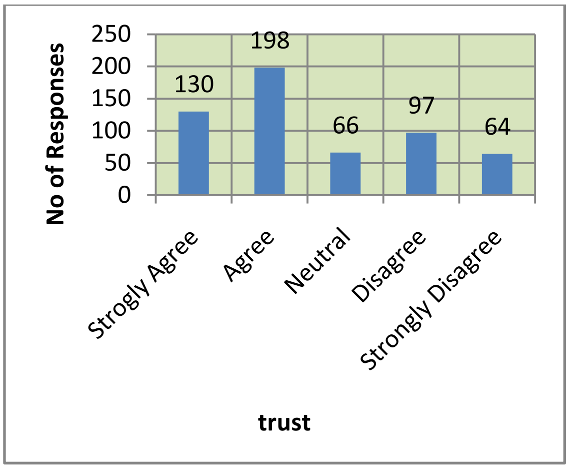

Figure 4: Trust among the hospital employees is important for the hospital information security

For the statement: 'There is a lack of trust amongst the employees due to a lack of an effective hospital culture'. The vast majority, 302 out of 588, strongly disagreed or disagreed with the statement, and only 173 out of 558 strongly agreed or agreed, as shown in figure 5.

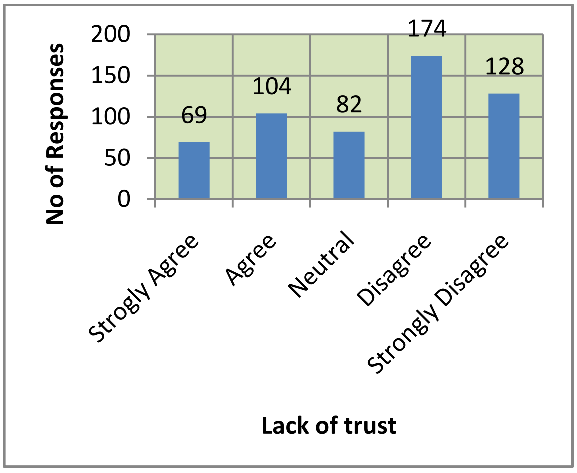

Figure 5: Lack of trust amongst the employees due to lack of effective hospital culture

For the Research Hypotheses:

Hypothesis 1: H1: Organization leadership positively related to the employees attitude toward health information security.

The research found that there is a positive relationship between the hospital leadership and information security culture with the hospital working environment. The qualitative data analysis is supporting such a relationship. It indicated that Saudi leadership is impacted by the Saudi Arabian national culture and reflected in the leadership management style, decision making and behaviour towards the information security culture.

Hypothesis 2: H2: Employees job satisfaction and job security is positively related to the employees' attitude toward information security.

Employees' job satisfaction has a positive relationship with the employees' attitudes towards information security behaviour. Job satisfaction in the hospital plays a major role in the employees' behaviour towards the information security culture. The qualitative data indicated that unsatisfied employees have less discipline towards complying with a positive information security culture. This is mentioned clearly as being evident amongst Saudis who are unsatisfied with their jobs and work in administration in the hospitals.

Hypothesis 3: H3: Trust is positively related to the employees' attitude toward information security.

There is a positive relationship between employees' trust and their attitudes towards information security culture. Trust helps in complying with the hospital's procedures and regulations with the hospitals. Trust also helps in positive behaviour with the hospital.

Hypothesis 4: H4: Organisation information security policy is positively related to the employees' attitudes towards information security.

The research confirmed that the organisation policy is positively linked between organisation information security policy and information security culture within the hospitals. The qualitative analysis indicated that having an IS policy helps in developing a positive information security culture.

Hypothesis 5: H5: Organisation communication is positively related to the employees' attitudes towards information security.

The research found that there is no link between the communication system and the information security culture within the hospitals. It is important to note however, that the qualitative analysis indicated that having a communication system helps in developing a positive information security culture.

Hypothesis 6: H6: Employees' intention towards information security is positively related to the employees' attitudes towards information security.

The research confirmed a strong relationship between employees' intentions and their attitudes towards information security. Attitude plays a major role on the employees' intention to use the information within the hospital. Having a positive attitude helps employees in complying with information security rules and procedures and improving the information security culture. On the other hand, having a negative attitude can lead to abusing the information security i.e, employees' behave negatively regarding information security.

Hypothesis 7: H7: Employees' intentions are positively related to their actual behaviour towards information security.

The research indicated that a positive relationship between employees' intentions to behave towards information security to the actual behaviour. The employees who have the intention to pass along medical information to a third party, for example, will do so in practice.

8. CONCLUSION

Effective information security helps in improving and promoting health services. This study investigated and analysed the role and impact of cultural dimensions on information security in Saudi Arabia health service. Two surveys were carried out in order to collect data and information from three major hospitals in Saudi Arabia (SA). The first survey identified the main cultural-dimension problems in SA health services and developed an information security culture framework model. The second survey evaluated and tested the developed framework model to test its usefulness, reliability and applicability. The model is based on human behaviour theory, where the individual's attitude is the key element of the individual's intention to behave as well as of his or her actual behaviour. The research identified six cultural dimensions: Saudi national culture, Saudi health service leadership, employees' trust, technology, multicultural interactions and employees' job roles. The research also identified a set of cultural sub-dimensions. These include working values and norms, tribe values and norms, attitudes towards women, power sharing, vision, social interaction, respect and understanding, hospital intra-net, hospital employees' language(s) used, multi-national culture, communication system, employees' job satisfaction and job security. The research identified that (a) the human behaviour towards medical information in SA is one of the main threats to information security and one of the main challenges to SA health authority, (b) The current situation of SA hospitals' IS cultures is falling short in protecting medical information due to the current value and norms towards information security, (c) Saudi national culture and employees' job role are the main dimensions playing major roles in the employees' attitude, and technology is the least important dimension playing a role in the employees' attitudes.

9. REFERENCES

[1] Marchibroda, J.M. (2007). "Health Information Exchange Policy and Evaluation, Journal of Biomedical Informatics", vol. 40, No 6, pp. 11-16.

[2] Eloff, J.H.P and Eloff, M. (2003). "Information Security Management-A New Paradigm", in proc. of The 2003 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on Enablement through Technology (SAICSIST 2003), pp. 130-136.

[3] Da Veiga, A. and Eloff, J.H.P. (2010). "A framework and assessment instrument for information security culture", Computers & Security, vol. 29, no 2, pp. 196-207, 2010.

[4] Hofstede, G. (1980) "Culture's Consequences: International Differences in Work-Related Values. London: Sage Publications.

[5] Hofstede, G. (2001). "Culture's Consequences: Comparing Values, Behaviors, Institutions, and Organisations across Nations. London: Sage Publications.

[6] Stedham, Y. and Yamamura, J. (2004). "Measuring national culture: Does gender matter?" Women in Management Review, 19(5), pp. 233-243.

[7] Huang, D., Rau, P.P. and Salvendy, G. (2007). "A survey of factors influencing people's perception of information security". In J. Jacko (Ed.), Human-Computer Interaction, Part IV. Heidelberg: Springer.

[8] Schultz, E. (2005). "The human factor in security". Computers and Security, 24, 42-426.

[9] Lacohee, H., Phippen, A. D. and Furnell, S. M. (2006). "Risk and restitution: Assessing how users establish online trust". Computers and Security, 25, 486-493.

[10] Chan, M., Woon, I. & Kankanhalli, A. (2005). "Perceptions of information security at the workplace: Linking information security climate to compliant behavior". Journal of Information Privacy and Security, 1(3), 18-42.

[11] Rotvold, G. (2008). “How to Create a Security Culture in Your Organization?” The Information Management Journal, 33-38.

[12] Thomson, K., and von Solms, R. (2005). “Information Security Obedience: A Definition”. Computers & Security, 24(1), 69-75.

[13] Siponen, M., & Oinas-Kukkonen, H. (2007). “A Review of Information Security Issues and Respective Research Contributions. SIGMIS Database, 38(1), 60-80.

[14] 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.

[15] Henderson A., Briggs, J., Schoonbeek, S. and Paterson, K. (2011). “A framework to develop a clinical learning culture in health facilities: Ideas from the literature”. International Nursing Review, 196-202.

[16] Pearcey, P. (2007). “Tasks and routines in 21st century nursing: Student -nurses’ perceptions”. British Journal of Nursing, 16(5), 296-300.

[17] Ruighaver, A.B., Maynard, S.B. and Chang M. (2007). “Organisational security culture: Extending the end-user perspective”. Computers and Security, 26, 56-62.

[18] Aldajani,M. (2012). “Electronic Patient Record Security Policy in Saudi Arabia National Health Services”, PhD Thesis, De Montfort University UK.