

Culture Dimensions of Information Systems Security in Saudi Arabia National Health Services

Saleh Alumarán, Giampaolo Bella, Feng Chen

Abstract—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. 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 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 a set of cultural and sub-cultural dimensions in SA health information security and services.

Keywords—Behaviour theory, Culture dimensions, Electronic health records, Information security.

I. INTRODUCTION

ON a global scale, 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.

II. RESEARCH BACKGROUND

Saudi Arabian health services have seen rapid growth in recent years to cope with the estimated population of 26

Saleh Alumarán is a PhD student of School of Computer Science and Informatics, De Montfort University Leicester, UK (e-mail: saleh.alomran@hotmail.com).

Giampaolo Bella (Dr.) and Feng Chen (Dr.) are with School of Computer Science and Informatics, De Montfort University Leicester, UK.

million with an annual growth rate of 2.2%, [4], [5]. The growth in health services is needed to cope with population growth as well as citizens' understanding and awareness of their rights in receiving the appropriate healthcare services.

Almost 60% of hospitals in Saudi Arabia are managed, owned and controlled by the Saudi government, namely by the Ministry of Higher Education. The hospitals' main objectives include providing basic healthcare services to the national and non-national, Saudi Arabia has a large number of non-national work in its various industries. It is important to stress that Saudi Arabia has introduced and implemented mandatory health coverage for all expatriates working in Saudi Arabia, and they are in the process of implementing this coverage to Saudi nationals. The Saudi authority established the Council for Cooperative Health Insurance in 1999. The main role of the council is to introduce, regulate and supervise the implementation of appropriate health insurance strategies for the Saudi healthcare market, [4]. The main effect of such implementation is the pressure on the healthcare providers to avoid any legal dispute with insurance companies, such as regarding handling the patients' medical information records [6].

The Ministry of Health is under pressure from authority and pressure groups such as media to cope with high health service operations demands and sharp increases in budget requirements as well as to meet patients' and their family's needs and satisfactions. These pressures have led the Ministry of Health to give the regional directorates some of the authority in terms of planning, recruitment healthcare staff and contracting with healthcare providers within a certain budget.

It is also important to stress that the SA health authority is adopting e-health initiatives to improve the services that it provides [7]. One of the main challenges of the health services is the security of electronic patient records and the necessity to save 10-15% of the public health budget [8].

III. PROBLEM STATEMENT

One of the main problems in SA healthcare services is the lack of clear and effective regulation to protect electronic patient records and implement appropriate policies to protect them [8]. This leads to the importance and the necessity for research in providing academic evidence to enhance and promote health information security. This research's main aims are to explore and identify health information security culture and provide appropriate framework to enhance information security.

IV. RESEARCH QUESTIONS

This study's main findings aim to provide answers and clear explanations to the following research questions:

- Q1. What is the current situation of information security culture in SA national health services?
- Q2. What are the main cultural dimensions and sub-dimensions influencing the information security culture of Saudi national health services?
- Q3. What is the structure of the information security culture

framework model?

- Q4. How reliable, practical and useful is the framework to Saudi Arabia's national health services?

V. HYPOTHESES

The research main hypotheses are as follows:

- H1. Organisational leadership is positively related to the employees' attitude towards health information security.
- H2. Employees' job satisfaction and job security are positively related to the employees' attitudes towards information security.
- H3. Trust is positively related to the employees' attitudes towards information security.
- H4. Organisations information security policies are positively related to the employees' attitudes towards information security.
- H5. Organisations' communication is positively related to the employees' attitudes towards information security.
- H6. Employees' intentions towards information security are positively related to the employees' attitudes toward information security.
- H7. Employees' intentions and their actual behaviour are positively related to information security.

VI. RESEARCH METHOD

A. Literature Survey

The first step in this research is to critically review the related literature. This is needed to develop the initial framework of the research and to benefit from other research related to the research topics to cover the research objectives.

B. Data Collection

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.

C. 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. The model 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.

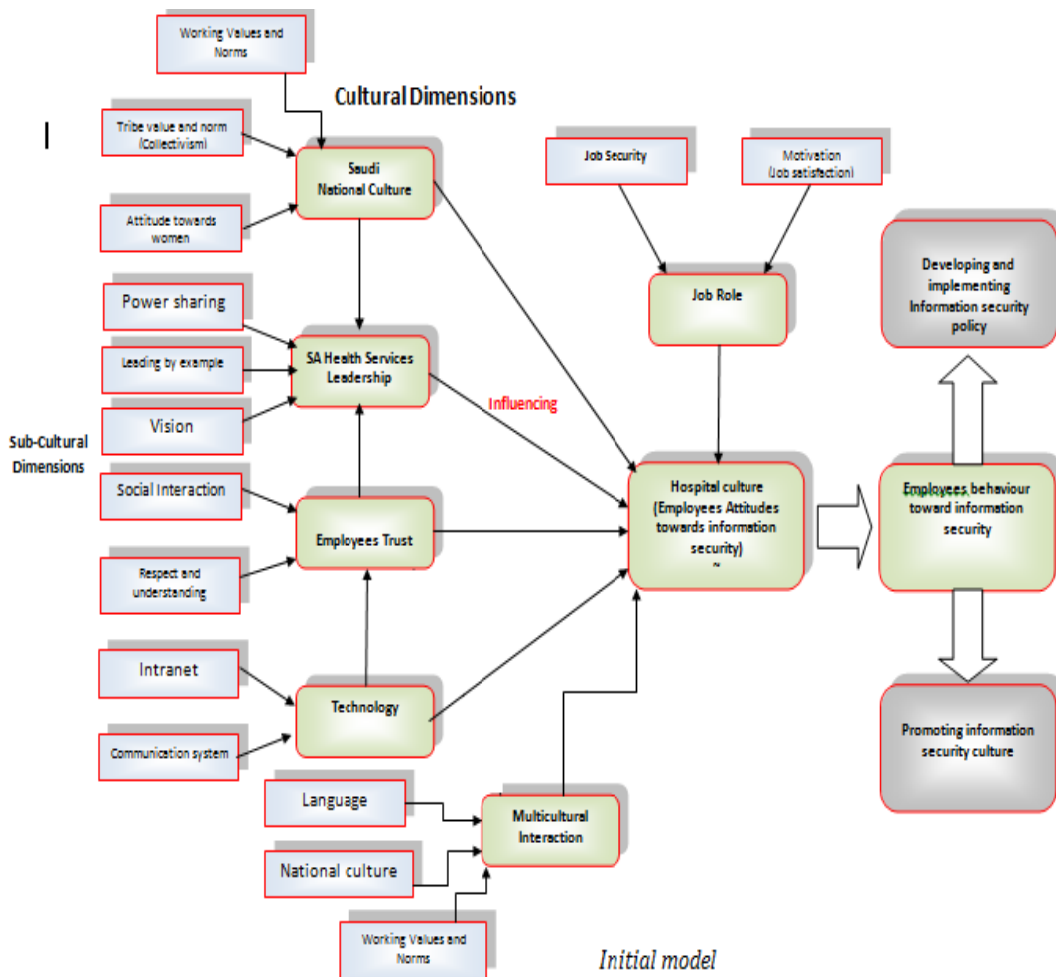


Fig. 1 Information Security Culture Model

VII. INFORMATION SECURITY CULTURE MODEL

A framework model for the information security culture for Saudi Arabia National Health Service has been developed and illustrated in Fig. 1. The model is based on human behaviour theory, which is based on the employees' attitudes towards information security, which play a major role on the individuals' use and misuse of information in health services. The intention to use the hospital information such as patient's information can lead to the actual use of the information. The model illustrates that six of culturally based dimensions contribute to the individual health services' staff members' attitudes towards information security. These six dimensions are as follows: Saudi national culture leadership, trust, technology, multi-cultural interactions in the hospital, and job satisfaction. These dimensions contribute to staff attitudes, which lead to the establishment of a distinctive organisation culture. Each dimension identified has its own sub-cultures. The sub-cultural dimensions are the main drives for the cultural dimension, as shown in Fig. 1.

VIII. 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 Statements

- '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.
- '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.
- '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.
- '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.
- '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.
- '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.
- '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.

- '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.
- '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.
- '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 Hypotheses:

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.

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.

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.

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.

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.

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.

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.

IX. 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.

REFERENCES

- [1] J. M. Marchibroda, "Health Information Exchange Policy and Evaluation, *Journal of Biomedical Informatics*", vol. 40, No 6, pp. 11-16, 2007.
- [2] J. H. P. Eloff and M. Eloff, "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)*, 2003, pp. 130-136.
- [3] A. Da Veiga and J. H. P. Eloff. "A framework and assessment instrument for information security culture", *Computers & Security*, vol. 29, no 2, pp. 196-207, 2010.
- [4] S. Walston, Y. Al-Harbi, B. Al-Omar, "The changing face of healthcare in Saudi Arabia", *Annals of Saudi Medicine*, vol. 28, pp.243-250, 2008.
- [5] M. Almalki, G. Fitzgerald and M. Clark, "Health care system in Saudi Arabia: an overview", *Eastern Mediterranean Health Journal (EMHJ)*, vol. 17, no. 10, pp. 784-793, 2011.
- [6] Colliers international. "Kingdom of Saudi Arabia Healthcare Overview", 2012, <http://www.colliers.com/~media/Files/EMEA/emea/research/speciality/2012q1-saudi-arabia-healthcare-overview.ashx>
- [7] M. Househ, M. Al-Tuwajjiri and B. Al-Dosari, "Establishing an Electronic Health Center of Research Excellence (E-CORE) within the Kingdom of Saudi Arabia", *Journal of Health Informatics in Developing Countries (JHIDC)*, vol. 4, no. 1, pp. 42-46, 2010.
- [8] M. Aldajani, "Electronic Patient Record Security Policy in Saudi Arabia National Health Services", PhD Thesis, De Montfort University UK, 2012.