The African Journal of Information Systems

Volume 3 | Issue 3 Article 1

10-2011

Information Security Culture in Public Hospitals: The Case of Hawassa Referral Hospital

Temesgen Gebrasilase
Technical & Vocational Education & Training, Hawassa, Ethiopia, temegebra@gmail.com

Lemma Ferede Lessa
Addis Ababa University, lemma.lessa@gmail.com

Information Security Culture in Public Hospitals: The Case of Hawassa Referral Hospital

Research Paper

Volume 3, Issue 3, October 2011, ISSN 1936-0282

Temesgen Gebrasilase
Hawassa TVET College, Ethiopia
temegebra@gmail.com

Lemma Lessa
Addis Ababa University, Ethiopia
lemma.lessa@gmail.com

(*Received May 2011, accepted September 2011*)

ABSTRACT

Information security culture is mainly considered as a set of information security characteristics that the organization values. In this paper, an attempt has been made to assess the information security culture of Hawassa Referral Hospital located in the south central part of Ethiopia. The study aimed at identifying determinant factors or issues impacting the implementation of an effective culture of information security in the hospital with an intention of improving the existing information security practice in the hospital. To that end, an information security culture assessment model and instrument were adopted from previous studies. The instrument (customized for the current study) incorporates statements that assess the knowledge, attitude, belief and actions of health care providers, and medical students in relation to information security culture. The case study indicated that there is a serious problem of information security culture at different levels in the hospital. Accordingly, identifying the current practices regarding information security in the hospital has a practical contribution in that it has direct implications on setting priorities in relation to information security in the hospital and strengthening different efforts on the issue throughout the health sector in the country. Recommendations are also provided as to how the hospital should approach the different factors and issues in order to put in place better and more secure information environments in the hospital.

Keywords

Information security culture; Information security; information security awareness

INTRODUCTION

Information security is 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 (Alnatheer & Nelson, 2009). Likewise, Martins & Eloff (2006) broadly defined Information security culture as a set of information security characteristics that the organization values; the assumption about what is acceptable and what is not in relation to information security; the assumption about what information security behavior is encouraged and what is not; and the way people behave towards information security in the organization.

The issue of information security is becoming more and more crucial in today's information age as the privacy and security issues of information resources face lots of challenges due to several factors such as the development of Information Technology. As presented by Von Solms (2000), so far there are four different waves of development of information security. The First Wave was characterized by Information Security being a technical issue, best left to the technical experts; the Second Wave was driven by the realization that information security has a strong management dimension, and that aspects like policies and management involvement are very important; the Third Wave consisted of the need to have some form of standardization of information security in a company, and aspects like best practices, certification, an information security culture and the measurement and monitoring of Information Security became important; and the Fourth Wave that of information security Governance.

In relation to ensuring security of information resources, the technological methods (such as firewalls and password) of protecting information may be effective in their respective ways; however, many losses are not mainly caused by lack of technology or faulty technology but rather by users of technology and faulty human behavior (Dhillon, 2001). Although many organizations have implemented technical solutions to protect information resources from adverse events, internal security breaches continue to occur. That is why human actions account for a far greater degree of computer-related losses than all other sources combined and this is why it is recently being argued that people must be an integral part of any organization's information security defense system (Kevin, 2007).

Studies have also shown that non-technical issues are as important as technical issues in safeguarding an organization's sensitive information (Dhillon and Torkzadeh, 2006; Siponen and Oinas-Kukkonen, 2007).Technical security controls are strong but they have to be correctly specified, designed, developed, implemented, configured, used and maintained - steps which all involve human beings. Simply put, security-aware managers, staff and information technology professionals make better use of technical security controls (Rotvold, 2008). Protecting information used in the wider context should therefore also incorporate the behavior of people. People manage the information in an organization and interact with information technology systems. In line with this Williams (2009) noted that the human component is a significant factor in information security, with a large number of breaches occurring due to user error. Technical solutions can only protect information so far and thus the human aspect of security has become a major focus for discussion. Therefore, it is important for organizations to create a security conscious culture. Hence, a positive information security culture can aid in minimizing the people threat compromising information security while interacting with information technology systems (Eloff and Von Solms, 2000).

In a recent study, Appari &Johnson (2010) indicated that Information security and privacy is an issue of growing importance in the healthcare sector. They further pointed out that adoption of digital patient records, increased regulation, provider consolidation and the increasing need for information exchange between patients, providers and payers, all point toward the need for better information security.

As to investigating information security, Ruighaver (2007) pointed that it should not only be investigated in a simplistic manner focusing on end-users and on the technical aspects but also it should

have a management focus as it is a management problem. Therefore, in this research an attempt is made to assess the information security culture of Hawassa Referral Hospital (located in south central part of Ethiopia) in order to help the hospital understand factors and issues that would help to bring an adequate and acceptable level of information security culture and practices.

This study will address the following research questions:

1. Is there awareness among health care providers and other administrative staffs about information security in Hawassa Referral Hospital?
2. Are there established cultures, mechanisms and procedures for protecting information and information assets in Hawassa Referral Hospital?
3. Does the management have the commitment and support for the implementation and incorporation of information security culture in Hawassa Referral Hospital?
4. Does the hospital have a proper policy and administrative control for protecting their information resources?

LITERATURE REVIEW

The literature holds information on the importance of information security culture in organizations. Among these are the need to have an effective organizational information security culture where employees intuitively protect corporate information assets (Dojkovski et al, 2001); socio-cultural measures that support technical security methods (Schlienger & Teufel, 2003); issues in relation to transitioning towards an information security culture for organizations (Ngo et al.,2005); the fact that information security culture is often explained using a variety of theories and established principles from other research areas (Ngo et al., 2005).

Martins and Eloff (2006) also make clear that a certain level of information security culture is already present in every organization using IT, but this culture could be a threat if it is not on an acceptable level. The aim in assessing that culture is to advance it to an adequate level. This could then aid in minimizing internal and external threats to information in the organization. They further stated that people are the center of every activity. Protecting information used in the wider context should therefore also incorporate the behavior of people. People manage the information in an organization and interact with IT systems.

As briefly summarized by Alnatheer & Nelson (2009), literature in the area of security shows that research on information security culture is still in its early stages of development where several issues are still being identified and conceptualized. Culture has influenced the formation of many security measures, such as national security policy, information ethics, security training, and privacy issues. Schlienger & Teufel (2002) (quoted in Alnatheer & Nelson, 2009) discussed that security culture covers social, cultural and ethical measures to improve the security relevant behavior of the organizational members and is considered to be a subculture of organizational culture. Security culture should support all organizational activities in a way that information security becomes a natural aspect in the daily activities of every employee. In conclusion, the establishment of an organizational information security culture is a necessary for effective information security.

Each organization has its own information security culture similar to every person having their own personality. A positive information security culture can aid in minimizing the people threat compromising information security while interacting with IT systems (Diver, 2006). The behavior of

employees towards information must be acceptable and needs to be part of everyday life in the organization. Every organization also has certain information security practices, which are followed and incorporated into the working environment. To facilitate the above, it is necessary to cultivate an information security culture in the organization (Von Solms, 2000; Eloff, 2000). According to Martins and Eloff (2006), information security culture can be seen as the assumption about what is acceptable and what is not in relation to information security. It may not, for instance, be acceptable to leave crucial business information in an office area where anyone could access or read it. Information security culture can also emerge from encouraging acceptable information security behavior. An example could be that people are encouraged to report security incidents via the appropriate management channel.

Organizational behavior plays an important role in the development of an organizational culture. Through the culture it will be clear what behavior is accepted and encouraged and what is not. To establish the desired culture in an organization, it is necessary to take a look at the organizational behavior of the employees. The type of culture in an organization can have a direct impact on the behavior and actions of the organization's employees (Martins, 2000). In an organization with a bureaucratic culture, where everyone has to play by the rules, employees might follow the information security policy more strictly than in a less formal and individualistic culture (Yeats, 1996). Changing an organization's culture will in effect then also require the focus to be on changing ineffective behavior and procedures and not the organizational culture (Hellriegel, Slocum, & Woodman, 1998).

An information security culture needs to be available at different levels in an organization including individual level, group level and organizational level. As indicated in the information security model below, each of the three levels incorporate different key issues (Martins, 2008). At organizational level: policy and procedures, benchmarking, risk analysis, and budget are the key issues. At group level management: trust; and at the individual level awareness and ethical conduct are the key issues.

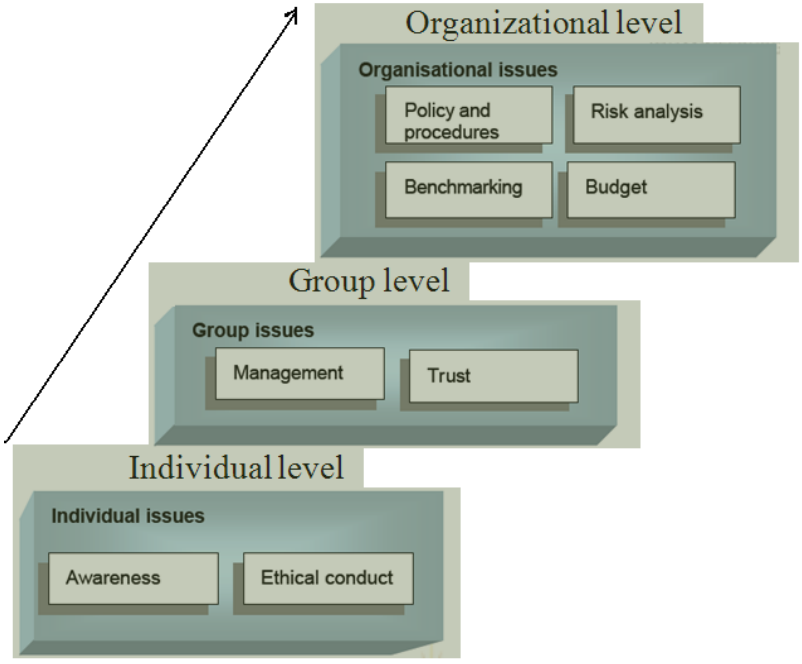

Figure 1: Basic information security culture model (Martins, 2008)

According to different research, the different factors and issues which influence information security culture and practices are classified: corporate citizenship, legal regulatory environment, corporate governance and cultural factors. The first factor is corporate citizenship, which is concerned with how employees gain an understanding of appropriate information security culture and practice through awareness raising and training programs. Senge (1990) refers to information security awareness as a state where users in an organization are aware of and are ideally committed to their security mission. Information security awareness is an important part of information security management (Nosworthy, 2000). Increasing awareness of security issues is the most cost-effective control that an organization can implement (Dhillon, 2001). Hinde (2002) suggests that the absence of awareness programs indicate a critical gap in effective security implementation. Kruger & Kearney (2006) also pointed out that due to the intensified need for improved information security, many organizations have established information security awareness programs to ensure that their employees are informed and aware of security risks, thereby protecting themselves and their profitability.

Legal and regulatory environment is another important factor that influences information security culture and practices. The major component of legal and regulatory environment is information security policies. The primary objective of information security policy is to define user rights and responsibilities in terms of information within an organization (Dhillon and Torkzadeh, 2006).

The third factor, corporate governance, includes factors and issues related to top management support for information security management and information security compliance. Top management support is seen as the most important factor affecting information security management activities in organizations (Fourie, 2003). In study by Knapp, Marshall, Rainer and Morrow (2004) 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 information security management is crucial, particularly for implementing information security policy. Culture is also another factor which has influenced the formation of many security measures, such as national security policy, information ethics, security training, and privacy issues (Chen and Medlin, 2008).

Specific to the health sector, privacy is viewed as a key governing principle of the patient-physician relationship and patients are required to share information with their physicians to facilitate correct diagnosis and treatment, and to avoid adverse drug interactions (Appari &Johnson, 2010). In such a case, patients may refuse to disclose important information in cases of health problems such as psychiatric evaluations and HIV/AIDS, as their disclosure may lead to social stigma and discrimination. For comprehensive classification of research in healthcare information security and privacy see Appari &Johnson (2010).

Dojkovski et al. (2001) indicated that the development of strong employee values was considered by all participants in their study to be an impossible challenge and it is found that recruiting people who already possess strong values is the only effective approach to create information security culture. Dhillon (2001) in his study has also suggested that organizations need to focus on the underlying beliefs that lead individuals to engage in intentional acts resulting in security breaches. Clearly, behavioral change is ultimately the result of changes in beliefs. Thus it is important that people within organizations are exposed to information which will produce changes in their beliefs. The findings of a study by Kraemer & Carayon (2005) also support the notion that information security culture is critical to the success or failure of overall Information System performance, operating at different levels and through various mechanisms. The results of the study provide a preliminary list of elements of several

Information Security culture dimensions. In another study by Tarimo et al.(2006) conducted in Tanzania, it is found that there is lack of personnel and resources to support information security education at colleges and universities which is one reason for lack of information security culture. Hence the study revealed that cultivating security culture is neither simple nor easy and information security is not an issue that could be addressed entirely by organizations alone; rather, many factors outside the scope of an organization have to be considered. Alnatheer & Nelson (2009) have also highlighted the importance of information security management factors and cultural factors in Saudi Arabia and the study disclosed a gap in terms of addressing the influences of both Information Security Management factors and cultural factors on the adoption of security culture in Saudi Arabia context.

METHODOLODY

The main aim of this research is to assess the information security culture of health care providers, administrative staffs and medical students in the area under consideration. To this effect, a descriptive survey research method was used.

This investigation was conducted in Hawassa Referral Hospital in Hawassa city. The hospital is the only referral hospital in Southern part of Ethiopia. According to the data obtained from the medical director office, the hospital provides medical services for more than 500 patients per day. It provides both medical services and teaching services in different health and medical departments.

A cross-sectional survey was used as a study design in this investigation which helped the researchers collect all the data and information from the selected sample at one time. The target population of this study were all health care providers (Nurses, Laboratory technicians, Pharmacists, etc), internship medical students, and administrative and supportive staffs who were primarily involved in health data gathering, processing and disseminating. According to the data obtained from the Human Resource Information Office of the hospital in March 2010, there were 306 health care providers and 120 administrative and support staff who were working in Hawassa Referral Hospital. In addition, the data obtained from Hawassa University Medicine Department indicates that there were 138 internship clinical and medical students. The sum of the target population of the study was 564.

To select respondents from the target population of the study, stratified sampling technique was employed. The reasoning is that the respondents do vary in their educational qualification, profession, exposure to health information in hospital, and so on. Thus, the target population is heterogeneous. As shown in the table below, the respondents were taken proportionally from each stratum. To select respondents from each stratum, a simple random sampling technique (lottery method) was used. The reasoning is that it gives equal chance for all respondents in each stratum. Added to this, it enhances the representatives of the sample drawn from each stratum.

Both qualitative and quantitative research approaches were found to be relevant in this study to gather data. Dawson (2006) described that each of these methods has its own weakness and strengthens but it is proper to use each instrument as long as it fits the purpose, size and situation under which the research is being conducted. In the quantitative approach, the investigator found the questionnaire of Martins (2008) very relevant for assessing the information security culture in the hospital. This questionnaire was used because it incorporates key information security culture issues such as information security policy, procedures, benchmarking, risk analysis, budget, management commitment, individual awareness and ethical conduct which are described in the information security model. In addition to this,

its usefulness and practicality had already been tested in different studies in developing countries including South Africa. This instrument was translated in to 'Amharic' to make questions brief and clear to respondents and the data collection was conducted with the 'Amharic' version of the questionnaire for the entire respondent. Since this research focused on the study of socio-cultural issues, it was equally important to use the qualitative approach. As a result, the investigator developed and used in-depth interview questions to obtain detail and additional information from the respondents. In addition to this, the data gathered through in-depth interviews and questionnaires was also supplemented by reviewing such documents as information security policy, strategic plan and annual financial report of the hospital. The quantitative data was integrated, summarized and analyzed by using SPSS version 15.0 while the qualitative data was analyzed manually.

Before the information security culture questionnaire and the in-depth interview questions were used on the study site, they were pre-tested on a small sample of health care providers and medical students in Black Lion Specialized Hospital in Addis Ababa to allow the researchers to understand the anticipated reaction of the larger group and to revise or restructure questions where necessary.

RESULTS and ANALYSIS

The attitude, belief and actions of employees towards information must be acceptable and needs to be part of the everyday life of the organization. Assessing the attitude and knowledge of employees towards information security helps the organization to understand the behaviour of employees with regard to information security and to identify issues that would assist the organization to implement and incorporate information security culture and practice. The main aim of this research was to assess the attitude and knowledge of Hawassa Referral Hospital health care providers, administrative employees and medical students toward information security.

A total of 311 respondents were included for the final analysis of the quantitative study. During the data collection, it was difficult to get completed questionnaires on time especially among health care providers and medical students mainly due to workload while on duty. As a result, a total of 39 questionnaires were excluded from the final quantitative analysis because of the incompleteness in response from the respondents. From the total of 311 respondents, 201(64.6%) of the respondents were males and the other 110(35.4%) were females. The age of the respondents ranged from 20 to 60 years with the median age of 26 and mean of 26.85. Of the total medical students who participated in this study, 32(33.3%) were internship medical students, 34 (35.4%) were clinical year medical students, while the remaining 30(31.3%) were emergency surgery.

Knowledge to information security

The information security culture questionnaire is divided into three sections (Martins, 2000): (1) Information security culture statements, (2) knowledge questions and (3) biographical questions. The first phase of this quantitative analysis involved determining how much knowledge employees have about information security issues.

	STATEMENT	YES	NO
1	I know what the term information security implies.	103(33.1%)	208(66.9%)
2	I am aware of information security related to my job.	47(15.1%)	264(84.9%)
3	I know a person or a team responsible for information security in the hospital.	8(2.6%)	303(97.4%)
4	The hospital has an information security plan.	30 (9.6%)	281(90.4%)

Table 1: Responses on five knowledge questions

As indicated in Table 1, respondents were asked if they know what the term information security implies. As can be seen from the above table, 264 (66.9%) of 311 respondents answered that they do not know what the term information security implies and the remaining 103(33.1%) of 311 participant answered that they know what the term information security implies. The above table also illustrates that 264 (84.9%) of 311 participant answered that they do not know information security related to their job while the remaining 47(15.1%) of 311 respondents know information security related to their jobs. A result from the above table also shows that, overwhelming majority of respondents that constitute 303 (97.4%) of 311 don't know a person or a team responsible for information security in the hospital while the remaining 8(2.6%) of 311 knows the existence of a person or a team responsible for information security. Table 2 also shows that 281 (90.4%) of 311 respondents answered that they do not know the existence of information security plan and the remaining 30(9.6%) of 311 participant answered that they know about the existence of information security plan.

Management of Information Security

This dimension includes the willingness to change working practices to ensure the security of information assets and an acceptance of a responsibility towards information security and necessities of resources.

	Statements	Strongly Disagree	Disagree	Unsure	Agree	Strongly Agree
1	I am prepared to change my working practices in order to ensure security of information.	34(10.9%)	49(15.8%)	28(9.0%)	90(28.9%)	110(35.4%)
2	It is important to budget annually for information security spending/coast.	19(6.1%)	29(9.3%)	54(17.4%)	108(34.7%)	101(32.5%)
3	I have a responsibility towards information security in the hospital.	128(41.2%)	102(32.8%)	10(3.2%)	58(18.6%)	13(4.2%)
4	All information about the hospital should be available for non-employee.	104(33.4%)	100(32.2%)	59(19.0%)	22(7.1%)	26(8.4%)
5	All information about the hospital should be available for employee.	40(12.9%)	54(17.4%)	38(12.2%)	90(28.9%)	89(28.6%)

Table 2: Responses on Information security management

Table 2 shows statements on information security management and it summarizes the response of the research participants on the information security culture statements related to the management of information security. When asked about the importance of allocating specific budget for the operation of information security, 209(67.2%) of 311 respondents replied 'agree' or 'strongly agree'. However, a considerable number of respondents 54(17.4%) of 311 respondents replied 'unsure' to the statement whereas 48(15.4%) replied 'strongly disagree' or 'disagree'. Regarding preparations to change their working practice in order to ensure the security of information, 200(64.3%) of 311 respondents replied 'strongly agree' or 'agree' to the statements. However, 28(9.0%) of 311 respondents said 'unsure' while the remaining respondents 73(26.7%) of 311 respondents 'strongly disagree' or 'disagree' to the statement.

Regarding the third item, the majority of the respondents that constitute 230(74.0%) of 311 respondents replied 'strongly disagree' or 'disagree' while 10 (3.2%) of 311 respondents said 'unsure' to the statement that reads 'I have a responsibility towards information security in the hospital' where as the rest of respondents 'agree' or 'strongly agree' to the above statement. Concerning the availability of information to employees outside of the hospital, the majority of the respondents that constitutes 204(65.6%) of 311 respondents replied 'strongly disagree' or 'disagree'. Among the rest of respondents, 59(19.0%) of 311 them replied that they are 'unsure' about the statements while 48(15.5%) of 311 them said 'agree' or 'strongly agree'. It can be understood that majority of the respondents do not believe information about the hospital should not be available to outside employee. With respect to the availability of hospital information to employee, significant number of the respondents 179(57.5%) of 311 replied 'strongly agree' and 'agree'. But the rest of respondents i.e. 94(30.3%) of 311 and 38(12.2%) of 311 respondents replied 'strongly disagree' or 'disagree' and 'unsure' to the availability of hospital information to employee respectively.

Communication

The information security cultural statements included in this dimension focus on aspects such as the explanation and communication of information security policy and informing people about what is expected of them regarding information security.

	Statements	**Strongly Disagree**	**Disagree**	**Unsure**	**Agree**	**Strongly Agree**
1	I am trained in the information security controls I am supposed to use.	144(46.3%)	100(32.2%)	47(15.1%)	11(3.4%)	9(3.0%)
2	Management communicates information security information on a need to know basis to all job levels.	98(31.5%)	123(39.5%)	79(25.4%)	6(1.9%)	5(1.7%)
3	I can easily obtain a copy of the information security policy.	128(41.2%)	64(20.6%)	104(33.4%)	7(2.3%)	8(2.6%)

Table 3: Responses on communication on Information Security

Table 3 summarizes the responses of participants on information security training and other communication issues in the hospital. To start with, respondents were asked to give their response if

they have received training on information security. Overwhelming majority of the respondents that constitute 244 (78.5 %) of 311 'strongly disagree' or 'disagree' to the statements while 20 (6.4%) of 311 respondents 'agree' or 'strongly agree' to the statement. The rest of the respondents, on the contrary, replied 'unsure' to the statement. It can be learned that the majority of the respondents reported that the hospital didn't conduct information security awareness training. While information security awareness training is an important tool for creating as well as sustaining information security culture, it is ignored in the hospital. As to the statement 'Management communicates information security information on a need to know basis to all job levels' in Table 3, majority of the respondents 221 (71.0%) of 311 'strongly disagree' or 'disagree'. The rest of respondents that constitute 79(25.4%) of 311 and 11(3.6 %) of 311 respondents responded 'unsure' and 'agree' or 'strongly agree' to the statement respectively.

In relation to access to a copy of information security policy in the hospital, the majority of the respondents that constitute 192 (61.8%) of 311 'strongly disagree' or 'disagree' and responded that they can't easily obtain a copy of information security policy easily. On the other hand, 104 (33.4%) of 311 respondents were 'unsure' about the statement whereas 15 (4.9%) of 311 research participant 'agree' or 'strongly agree' to the statement and believed that they can easily obtain a copy of information security policy.

Governance

This factor focuses on aspects such as whether management supports the information security policy, the adequate protection of information asset, the perception of the importance of information security and adequate control over information assets.

	Statements	**Strongly Disagree**	**Disagree**	**Unsure**	**Agree**	**Strongly Agree**
1	It is important to determine the hospital's information security needs.	3(1.0%)	4(1.3%)	3(1.0%)	81(26.0%)	220(70.7%)
2	Information security should be regarded as a functional (business) issue.	132(42.4%)	30(9.7%)	89(28.6%)	14(4.5%)	46(15.0%)
3	Information security should be regarded as a technical issue.	181(58.2%)	91(29.3%)	8(2.8%)	16(5.2%)	15(4.8%)
4	I think it is important to implement information security in the hospital.	4(1.3%)	18(5.8%)	30(9.7%)	100(32.2%)	159(51.2%)
5	Management assists in the implementation of information security issues.	94(30.2%)	80(26.0%)	114(36.7%)	12(3.9%)	11(3.5%)
6	Management perceives information security as important.	114(36.7%)	116(37.3%)	54(17.4%)	11(3.5%)	16(5.1%)
7	Procedures are implemented to support the information security policy.	140(45.0%)	84(27.0%)	72(23.2%)	6(1.9%)	9(3.0%)

Table 4: Responses on perception and commitment of management

Table 4 summarizes the responses of participants on the perception and commitment of management towards the implementation of information security and the perception of employee towards the importance of information security. To begin with, participants were asked if it is important to determine the organization information security needs. Accordingly, significant number of respondents that constitute 301 (96.8%) of 311 'strongly agree' or agree whereas 3 (0.96%) and 7 (2.25%) of 311 of the respondents said 'unsure' and 'disagree' respectively. Regarding the fourth item in table 5.5, 259 (83.4%) of 311 respondents 'strongly agree' or 'agree' to the statement and reported that it is important to implement information security in hospital whereas 30 (9.7%) of 311 and 22 (7.1%) of 311 of the respondents said 'unsure' and 'strongly disagree' or 'disagree' respectively.

The research finding, as shown in Table 4, also revealed that majority of the respondents (56.0%) 'strongly disagree' or 'disagree' to the management support in implementation of information security policy in the hospital. On the other hand, 36.7% respondents are 'unsure' while 7.4% 'agree' or strongly agree' as to the availability of management support on the implementation of information security policy. Concerning the perception of the management about the importance of information security, the majority of respondents that constitute 230 (74.0%) of 311 replied 'strongly disagree' or 'disagree'. Among the rest of respondents, 54 (17.4%) of 311 replied 'unsure' while 27 (8.6%) of 311 respondents 'agree' or 'strongly agree' with the statement.

Participants were also asked if they consider information security as technical issue. Significant number of them that constitute 272 (87.5%) of 311 respondents 'strongly disagree' or 'disagree'. On the other hand, 8 (2.8%) of 311 respondents had 'unsure' position about the statement and 31 (7.1%) of 311 respondents replied 'agree' and 'strongly agree'. Regarding the second item, significant number of respondents that constitute 162 (71.0%) of 311 'strongly disagree' or 'disagree' while 89 (28.6%) of 311 said 'unsure' to the assertion. Only 60 (19.5%) of 311 respondents said 'agree' or 'strongly agree'. Concerning the implementation of procedures for supporting information security in the hospital, significant number of respondents that constitute 224 (79.6%) of 311 respondents 'strongly disagree' or 'disagree' whereas 72 (23.2%) of 311 and 15 (4.9%) of 311 respondents said 'unsure' and 'agree' or 'strongly agree' respectively.

Performance Accountability

Performance accountability focuses on aspects such as adherence to information security policy by various business areas and whether people should be held accountable for their actions if they do not adhere to the information security policy.

	Statements	Strongly Disagree	Disagree	Unsure	Agree	Strongly Agree
1	I adhere to the hospital's information security policy.	28 (9.0%)	50(16.0%)	179(57.6%)	30(9.6%)	24(7.7%)
2	I should be held accountable for my actions if I don't adhere to the information security policy.	110(35.4%)	90(28.9%)	28(9.0%)	49(16.0%)	34(10.9%)
3	The hospital ensures that I adhere to the information security policy.	114(36.7%)	100(32.2%)	69(22.2%)	10(3.2%)	18(5.8%)

Table 5: Responses on Performance Accountability

Table 5 above summarizes results concerning adherence to information security policy. Regarding their adherence to information security policy, 179 (57.6%) of 311 respondents replied 'unsure' to the statement. However, 78 (25.0%) and 54 (17.3%) replied 'strongly disagree' or 'disagree' and 'strongly agree' or 'agree' respectively. In table 5 it is also indicated that the majority of the respondents (68.9%) 'strongly disagree' or 'disagree' to the issue of performance accountability and believed that the organization do not have the mechanism for ensuring whether employees are adhering to the information security policy while 28 (9.0%) of 311 participants 'strongly agree' or 'agree' with the statements. The response of health care providers, medical and clinical students and other supportive staff on the second item in the table shows that 200 (64.3%) 'strongly disagree' or 'disagree' while 28 (9%) remained 'unsure'. It can be said that most of the respondents do not hold themselves accountable if they don't adhere to the information security policy.

DISCUSSIONS

One of the major findings of this study was the lack of awareness among health care providers, administrative staff and medical students about information security. In this study, it was found that 264 (66.9%) respondents responded that they do not know what the term information security implies. The study also showed that 264 (84.9%) of 311 respondents do not know information security issues related to their jobs. According to Hinde (2002), the absence of security awareness indicates a critical gap in effective security implementation. It was also showed that, overwhelming majority of the respondents that constitute 244 (78.5 %) of 311 'strongly disagree' or 'disagree' with the information security statement 'I am trained in the information security controls I am supposed to use'. In a similar manner, it is also possible to infer that the absence of information security awareness among the respondents may be caused by the absence of security awareness training in the hospital.

According to the study conducted by Deloitte and Thomatsu (2005), about 45% of global organizations do not sensitize their employees in respect to possible information security threats and this lack of information security awareness could well lead to compromised information within the organization. In the qualitative study, it was also indicated that there was lack of awareness among key informants about information security. In similar manner, it was also possible to infer that this lack of awareness might hinder the management to commit sufficient resources for information security operation and implementation. The study conducted by Rotvold (2008) also indicated that management awareness, commitment and support were a few of the more common reasons given for security awareness training not being conducted.

Our study also revealed that the majority of the respondents never received information security awareness training. As a result, the majority of the health care providers and other staff needed extra - information security awareness training and education. According to Dhillon (2001), increasing the awareness of security issues is the most cost-effective control that an organization can implement to bring effective information security culture. Training of security issues or features is an important tool for creating as well as maintaining security conscious behaviors.

Another important finding of this study was the lack of commitment and support by top management for the operation and implementation of information security. The study showed that 174 (56.2%) of 311 respondents 'strongly disagree' or 'disagree' with the information security culture statement which indicates the assistance of management for the implementation of information security. It is sound to infer that this lack of support by top management might be caused by lack of awareness about

information security. In studies by Knapp, Marshall, Rainer and Morrow (2007), it was indicated that top management support is ranked number one in a list of 25 information security issues affecting information security in the organization.

The highest level of respondents (92.8%) also reported that they do not know the existence of information security policy in the organization. This result was reaffirmed by the result obtained from the in-depth interview held with the medical director. Concerning this issue, the medical director confirmed the absence of a written information security policy in the hospital. According to the study conducted by Higgins (1999), without an information security policy, security practices would be developed without clear demarcation of objectives and responsibilities. Effective information security policies would help to define the users' right and responsibility in relation to information within the organization and help users to understand acceptable and responsible behavior in information resources. The presence of well written and documented information security policy also helps senior managers to control and monitor employee behavior in relation to information.

The establishment and implementation of information security policy alone does not ensure that employees will necessary obey these policies (Von Solms, 2004). In our study, it was indicated that more than half (57.6%) of the respondents are 'unsure' whether they are adhering to the organization information security policy or not. The study also showed that 68% of respondents reported that the organization do not have a mechanism for ensuring whether employees are adhering to the information security policy. In line with this, a study conducted by Karabacak (2006) underlined that organizations need to evaluate their information security compliance level and they should have a mechanism to ensure that the practice of employees is compliant with the information security policy particularly because a significant number of information security breaches result from employees failure to comply with security policies. As a result, policy enforcement is necessary and essential for the success of information security policy.

RECOMMENDATIONS

Short-term

- Implement information security awareness training program to bring information security conscious behaviors.
- Senior managers in the hospital should support and commit enough resources for the operation of information security in the hospital.
- Improving the existing information protection procedures in the hospital to bring adequate protection to information assets in the hospital.
- Developing information security guidelines that can guide employees to properly use information assets in the hospital.
- Assigning a specific person or team who can take full responsibility for information assets in the hospital.
- Implement awareness measures outside of the class or training room to help employees remember the lessons learnt.

Long-term

- Formulating health information security policy by involving all stakeholders from the health sector.
- Incorporation of information security topics or courses in the curriculum of health education at tertiary level.
- Federal Ministry of Health should incorporate information security as one core processes or function in the hospitals.

- Appropriate ICT infrastructure that can provide technical protection for information assets should be implemented.
- More studies on information security culture with broader scope are required to have detail insights about the issue in the health sector in the country.

REFERENCES

Alnatheer, M. & Nelson, K. (2009). Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context. *Proceedings of the 7th Australian Information Security Management Conference*, Perth, Western Australia.

Appari, Ajit & M. Johnson, Eric (2010) Information security and privacy in healthcare: current state of research. *Int. J. Internet and Enterprise Management, Vol. 6, No. 4.*

Dhillon, G. (2001). Violation of Safeguards by Trusted Personnel and Understanding Related

Information Security Concerns. *Computers & Security*; Vol.20, No.2, pp.165-172.

Dhillon, G. & Torkzadeh(2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*, 16, 293-314.

Dojkovski, S., Lichtenstein, S., & Warren, M. J. (2001) Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia; Available at: http://www.is2.lse.ac.uk/asp/aspecis/20070041.pdf (Accessed September 14, 2011).

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

Hellriegel, D., Slocum,J.W. & Woodman, R.W. (1998). *Organizational Behavior*. Eighth edition: South-Western College Publishing.

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

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

Kraemer, S., Carayon, P. (2005) Computer and Information Security Culture: Findings from Two Studies. *Proceedings of the Human Factor and Ergonomics Society 49th Annual Meeting.*

Kruger, H.A., & Kearney,W.D. (2006) A prototype for assessing information security Awareness. *Computers & security*, 25, 289–296.

Martins, A. (2000). The influence of organizational culture on creativity and innovation in a university library. M.Inf. Dissertation. Pretoria: University of South Africa.

Martins, A. (2008). Information security culture; DigiSpace at the University of Johannesburg; available at: http://ujdigispace.uj.ac.za:8080/dspace/handle/10210/292; viewed on Sept. 5, 2009.

Martins, A. & Eloff, J. (2006). *Assessing Information Security Culture*. Johannesburg, South Africa: Rand Afrikaans University.

Ngo, L., Zhou, W. & Warren, M. (2005) Understanding transition towards organizational culture change. *Proceedings of the 3rd Australian Information Security Management Conference*, Perth Australia.

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

Rotvold, Glenda (2008). How to create a Security Culture in Your Organization, Available at: http://content.arma.org/IMM/NovDec2008/How_to_Create_a_Security_Culture.aspx.

Ruighaver, A.B., Maynard, S.B., Chang, S. (2007) Organizational security culture: Extending the

end-user perspective. *Computers & security*, 26, 56–62.

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

Schlienger, T. & S. Teufel (2003) 'Information Security Culture - From Analysis to Change.' *Proceedings of ISSA 2003*, Johannesburg, South Africa, 9-11 July 2003.

Tarimo, C. N., Bakari, J. K, Yngström, L., & Kowalski, S. (2006) A Social-Technical View of ICT Security Issues, Trends, and Challenges: Towards a Culture of ICT Security - The Case of Tanzania Available at: http://www.citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.145.2850.pdf (Accessed September 20, 2011)

Von Solms, B. (2000). Information security – The third wave?. *Computers and Security*. 19(7), November: 615-620.

Von Solms, B. (2000). Information security – The Fourth wave?. *Computers and Security*. 25 (165), 165-168.

Williams, P. A. (2009) What Does Security Culture Look Like For Small Organizations? *7th Australian Information Security Management Conference*, Perth, Western Australia.