ADDIS ABABA UNIVERSITY

Faculty of Informatics

Health Informatics Program

ASSESSMENT OF INFORMATION SECURITY CULTURE IN PUBLIC HOSPITALS IN SOUTHERN NATIONS NATIONALITIES AND PEOPLES REGION/SNNPR/: THE CASE OF HAWASSA REFERRAL HOSPITAL

BY

TEMESGEN GEBRASILASE

June, 2010

ADDIS ABABA

ADDIS ABABA UNIVERSITY

Faculty of Informatics

Health Informatics Program

ASSESSMENT OF INFORMATION SECURITY CULTURE IN PUBLIC HOSPITALS IN SOUTHERN NATIONS NATIONALITIES AND PEOPLES REGION: THE CASE OF HAWASSA REFERRAL HOSPITAL

A thesis submitted to the school of graduate studies

Addis Ababa University

In partial fulfillment of the requirements for the Degree of Master of Science in Health Informatics.

Investigator:-Temesgen Gebrasilase

Adviser: - Ato Lemma Lessa

June, 2010

ADDIS ABABA

ADDIS ABABA UNIVERSITY

SCHOOL OF GRADUATE STUDIES

ASSESSMENT OF INFORMATION SECURITY CULTURE IN PUBLIC HOSPITALS IN SOUTHERN NATIONS NATIONALITIES AND PEOPLES REGION: THE CASE OF HAWASSA REFERRAL HOSPITAL.

By:-Temesgen Gebrasilase

Health Informatics Program

Faculty of Informatics, Addis Ababa University

Approved by the Examining Board

Mahder Alemayehu

Chairperson, Department Graduate Committee

Advisor

Lemma Lessa

Examiner

ERMIAS ABEBE

Acknowledgments

I am very grateful to my advisor Ato Lemma Lessa from the faculty of informatics, Addis Ababa University, for his unreserved guidance and constructive suggestions and comments from the stage of proposal development to the end.

My honest gratitude also goes to the medical director of Hawassa Referral Hospital and to the Ethical Review Board of Hawassa University Referral Hospital and to all staffs for their valuable support and assistance during data collection.

I am very grateful to Hawassa TVET College for their valuable support during my post graduate study. My honest gratitude also goes to Ayalew T. and Muluembete G. and Teshome A. for their constructive comment and other necessary support.

I take this opportunity to extend my thanks to all of my teachers in the Faculty of Informatics and School of Public Health, other administrative staffs and to all my friends in Hawassa for their encouragements and other necessary supports during my post graduate study and in the whole research processes.

Lastly, my thanks also go to my baby girl, my wife and to all my families for their valuable support, without them this research wouldn't have been possible.

Acronyms

ART	Anti-Retroviral Therapy
EU	European Union
HCPs	Health Care Providers
HRH	Hawassa Referral Hospital
ICT	Information Communication Technology
IT	Information Technology
KM	Kilo Meter
OPD	Out-Patient Department
SNNPR	Southern Nation Nationalities and People Region
SPSS	Statistics Package for Social Science
UK	United Kingdom
UN	United Nation
USA	United States of America
VCT	Voluntary Counseling and Testing

Table of content

List of tables

Abstracts

Background: - Traditionally, most of the researchers and experts in the field of information security believed a technological solution to address majority of information security issues. However, contemporary studies have shown that non-technical solutions including the human behavior and processes are as important as technical solutions in safeguarding organization information assets.

Objective: - To assess the information security culture of Hawassa Referral Hospital in order to improve the existing information security culture of the hospital.

Methods: - A cross-sectional survey was conducted in Hawassa Referral Hospital from March-April 2010. A total of 314 study subjects were participated for questionnaire and in-depth interview. The data was collected by using a non-structured pre-tested questionnaire, in-depth interview and document analysis. The quantitative data was analyzed by using SPSS version 15.0 and the qualitative data was analyzed manually.

Results: - It was found that, 66.9% of the study participants have no knowledge about information security. About 63% of the respondents reported that management does not assist to the implementation and incorporation of information security in the hospital. The result of the study also showed the absence of well written and documented information security policy in the hospital.

Conclusion and recommendations: - The study showed that majority of the respondents in the hospital has no knowledge about information security. The study also revealed that there is a lack of commitment from top management for the incorporation and implementation of information security in the hospital. Hence, it is recommended that there is a need to provide extra-education and training on information security issues for health care providers, administrative staffs and medical students. It is also recommended that the hospital management need to increase their support and commit enough resources to bring acceptable level of information security culture and practices in the hospital.

1. Introduction

1.1. Background

The technological methods 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 (Siponen, 2007). Rotvold (2008) says "People not only can be part of the problem, but also they can and should be part of the solution". People must be an integral part of any organization's information security defense system. Keeping information secure is not only the responsibility of information technology security professionals, but also the responsibility of all people within the organization (Hinson, 2009).

Guidelines for effective information security management practices are becoming prerequisite for organizations in order to promote the necessary steps to ensure successful outcomes. A good information security culture involves employees at all levels to ensure the security of data and physical assets. Studies indicate that awareness of security policies and procedures is considered as important mechanism to strengthen security practices in an organization. Organizations need to continue to be watchful about ensuring that their security policies and procedures are enforced and that educating employees remains a top priority (Rotvold, 2008).

Security awareness programs address the need to educate all people in an organization so that they can help to effectively protect the organization's information assets. 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 (Hinkle, 2007). Therefore, an approach that emphasizes an information security culture within the organization is required to make security as a part of employee's daily work routines. In order to develop a successful information security culture within an organization, it is a need to understand both technical and non-technical aspects of information security (Rotvold, 2008).

1.2. Statement of the Problem

According to the study conducted by Hong (2003), patient data collected and stored in hospitals and health care facilities is a prime target for malicious data hunters. Among the top reasons for this, the study found that lack of awareness within the health care industry around the frequency and seriousness of identity theft that negatively impacts efforts to control the problem and reduce the risk. According to Dawn and Andrew (2007), periodic security awareness training for all employees in most organizations is generally low to nil. A culture of security awareness is not encouraged in most organizations.

Information security risks have grown with the rapid growth in the number and types of people who have a legitimate interest in the information kept in medical records. Most importantly, the best known of many cases involve inappropriate access and disclosure of information contained in paper records or in widely accepted hospital information systems like those that report laboratory test results. These disclosures highlight the importance of the individual responsibilities of those handling confidential information and the critical requirement for education and monitoring of individuals with access to confidential material (Rotvold, 2008).

It is not practical for most organizations to implement 100% protection against every threat to every organizational resource. Therefore, it is important to adequately protect sensitive information. The threat environment under which the system operates needs to be understood in order to accurately assess organization security risk. Unfortunately, many organizations focus on protecting information from access or sabotage by those external to the organization and overlook insiders (Dawn and Andrew, 2007).

While employees obviously must have access to organization facilities and equipment, most do not need access to all areas of the workplace. Organizations should have a mechanism for controlling physical access for their information system. All access must be specifically granted to specific individuals. In particular, physicians and nurses should not have routine and unlimited access to the records of patients who are not under their care at the moment. Because most serious violations of privacy and confidentiality involve inappropriate behavior by individuals with authorized access, an essential feature of clinical information system security is the policy for dealing with violations (Dawn and Andrew, 2007).

Information security culture has been identified as the most important and critical aspects of information security. But it is not addressed very well in many researches. Hence, it is high time to study this issue. In line with this, lack of attention and awareness given by the health staffs concerning health information security in most health institution in Ethiopia is another focus of this investigation. In addition to this, this investigation is not studied in Ethiopian context and due to the aforementioned reason it is a high time to study information security culture.

This research aims in assessing the existing attitudes, belief, knowledge and actions of medical and non-medical staff about information security in Hawassa Referral Hospital/HRH/. It also aims to assess issues and factors which influence information security culture and practice in order to help organization to improve their information security culture.

This research will contribute a lot to alleviate the problems that the public hospitals in the SNNPR face in identifying factors or issues related to information security practices. The main beneficiaries of this research are public hospitals in the region. The outcome of the research may affect the way how the public hospitals address information security issues and also bring change in the policies, rules and guidelines in relation to information security. The investigator attempted to understand factors or issues that hindered the implementation of information security culture and practices in public hospitals in SNNPR, more specifically in HRH. More specifically, this study attempts to assess the attitude, belief, knowledge and actions of medical and non medical staffs towards information security and aims to answer the following questions:

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

1.3. Objective of the Study

1.3.1. General Objective

The general objective of this research is to assess the information security culture of Hawassa Referral Hospital in order to improve the existing information security culture of the hospital.

1.3.2. Specific Objectives

1. To assess the attitude and knowledge of health care providers and other administrative staffs towards information security.
2. To discuss factors and issues that facilitates the implementation and adoption of information security culture and practices in the hospital.
3. To recommend measures for improving information security culture and practices in public hospitals.

1.4. Significance of the Study

Primarily, this investigation serves physicians, nurses, laboratory technician, record officers and health facility managers as a reference for their further knowledge on information security culture. This research will also contribute a lot to alleviate the problems that the public hospitals in the region face in identifying challenges related to information security practices. This study also helps in filling the gap of human understanding on health information security culture and the different factors which helps the implementation and incorporation of information security culture. The study can also be a starting point for other researchers to study the issue in more detailed and wider geographical area in the country. It also serves policy maker or planner as additional reference for the formulation of national health information security policy. Specifically, the main beneficiaries of this research are

public hospitals in the region. The outcome of the research may affect the way how public hospitals address information security issues and also bring change in the policies, rules and guidelines in relation to information security in the institutions.

1.5. Scope of the Study

The study is delimited only to Hawassa Referral Hospital, which is found in Hawassa city. The hospital was selected based on personal experience of the researcher to the city. In addition to this, the complexity of the issue under investigation, size of the instrument and the item, limitation of the research time and financial resources and lack of research experience forced the researcher to delimit the study in the hospital.

1.6. Operational Definition of Key terms

Information Security: - According to Pfleeger (1997), information security is the preservation of the confidentiality, integrity, and availability of information and information resources.

Information Security Policy: - A security policy is a formal statement of the rules through which people are given access to an organization's technology, system and information assets (Weise, Joel and Martin and Charles, 2001).

Information Security Culture: - According to Martins and Eloff (2006), Information security culture is the assumption about what information security behaviors is encouraged and what is not.

Information Security Awareness: - Senge (1990) refers to information security awareness as a state where users in an organization are aware of, and ideally committed to, their security mission.

2. Review of Related Literature

2.1. Information Security

Access to high-quality, complete, accurate and up-to-date information makes managerial decision-making relatively easy by reducing the margin for error. Organizations design and build information systems that are effective at gathering, analyzing and outputting the information they need and secure information systems against risks to their confidentiality, integrity and availability. Now days it is not possible to assure 100% information security in an organization, however, a comprehensive and reliable information security controls reduce the organization's overall risk profile. Good information security builds management's confidence and trust (Rotvold, 2008)

Information security may be defined as the prevention of, and recovery from, unauthorized or undesirable destruction, modification, disclosure, or use of information and information resources, whether accidental or intentional. According to Pfleeger (1997), information security is the preservation of the confidentiality, integrity, and availability of information and information resources. Information security maintains three basic services: Preventing disclosure of information to unauthorized users (confidentiality), ensuring data cannot be modified without authorizations (integrity) and ensuring the availability of information to authorized users when they require them (Pfleeger, 1997).

It is important to adequately protect sensitive information. The threat environment under which the information system operates needs to be understood in order to accurately assess organization security risk. Unfortunately, many organizations focus on protecting information from access or sabotage by those external to the organization and overlook

insiders. It is imperative that organizations recognize the potential danger posed by the knowledge and access of their employees. Insider threats impact the integrity, availability, or confidentiality of information sensitive to an organization's and clients (Dawn and Andrew, 2007).

According to Deloitte's 2005 Global Security Survey (2005), organizations are now beginning to recognize that technology is an enabler, not the solution, for implementing and executing a sound security strategy. According to the above study, the top three success factors (i.e. management support of information security policies, users following information security policies and qualified security staffs) highlight the need for public and private entities to focus more time and attention on policies, processes and people, all areas which have been traditionally overlooked in favor of trusting hardware and software to solve security problems. 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 - all of which steps involve human beings. Simply put, security-aware managers, staff and information technology professionals make better use of technical security controls (Rotvold, 2008). Formal security policies, no matter how carefully they are written, are of little value unless employees know about them, understand their obligations and actively comply. Information security has to become second nature for employees i.e. an inherent part of the corporate culture, as natural as wearing a seatbelt in a car. The goal is to establish and maintain an organizational culture where information security is second nature to all employees (Deloitte, 2005).

Management needs to incorporate information security as one of the characteristics of the organization and demonstrate its commitment to, and involvement in, the processes of implementing it effectively. Management also needs to appoint a specific team or person to take responsibility for instilling the correct way in which things are done regarding information security (Martins and Eloff, 2006). Involving top management and getting their support is essential in building a strong security awareness that employees will take seriously. If management commitment is increased, and the security awareness goals and message are communicated and communicated often, progress and improvement can be made in creating a security culture (Rotvold, 2008).

2.2. Information Security Culture

Culture has influenced the formation of many security measures, such as national security policy, information ethics, security training, and privacy issues (Chen and Medlin, 2008). Security culture covers social, cultural and ethical measures to improve the security relevant behavior of the organizational members and considered to be a subculture of organizational culture (Schlienger and Teufel, 2002). Security culture should support all organizational activities in a way that information security becomes a natural aspect in the daily activities of every employee (Schlienger and Teufel, 2002). Security cultures assist the enforcement of information security policies and practices in the organization. As a result, each organization goal is to be able achieve an effective information security culture in their organization. Information security culture will emerge over time and become evident in the behavior and activities of the workforce (Martins and Eloff, 2006).

Organizational culture defines how an employee sees the organization (Ulich, 2001). It is a collective phenomenon that is growing and changing over time and, to some extent; it can be influenced or even designed by the management. The organizational culture is consequently expressed in the collective values, norms and knowledge of organizations. In turn, those collective norms and values affect the behavior of the employees. Schein (1999) defines organizational culture as the pattern of basic assumptions that a given group has invented, discovered, or developed in learning to cope with its problems of external adaptation and internal integration, and that have worked well enough to be considered valid, and, therefore to be taught to new members as the correct way to perceive, think, and feel in relation to those problems. Ultimately, the organizational culture has a crucial impact on the corporate success (Rühli, 1991).

Organizational culture emerges and grows with time. It is formed by the behavior of dominant organization members like founders and top managers. An organizational culture can have different subcultures based on sub organizations or functions. Information security culture is a subculture in regard to general corporate functions. It is the assumption about what information security behavior is encouraged and what is not. Information security culture will also emerge from encouraging acceptable information security behavior (Martins and Eloff, 2006). It should support all activities in a way, that information security becomes a natural aspect in the daily activities of every employee.

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 (Hellriegel, et al., 1998).

There is a little agreement on security culture definition or what exactly constitutes security culture. According to Martins and Eloff (2006), information security culture is the way people behave towards information security in the organization. People have their own attitudes towards different situations and processes in an organization. These attitudes could be positive or negative and have an impact on the way people behave. Their attitude towards information security and how they perceive it will result in certain behavior. They also defined information security culture as a set of information security characteristics that the organization values. These characteristics, such as integrity, confidentiality and availability of information, need to be valued and pursued by the organization.

Martins and Eloff (2006) made clear that certain level of information security culture is already present in every organization, 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. People invented information technology; they drive it, develop it, but also pose the most serious threat, whether intentional or unintentional, to information used in the information technology environment.

Studies in information security culture have shown that the establishment of an organizational information security culture is necessary for effective information security (Eloff and Von Solms, 2000). However, organizational culture may have a substantial influence on the security of information, and this could be negative or positive (Chang and Lin, 2007). It is imperative that the organizational culture reflects a positive attitude to information security in the entire organization (Schlienger and Teufel, 2003) and it is also important that organizational activities are consistent with good information security culture practices (Van Niekerk and Von Solms, 2005).

An information security culture has to have at all levels of an organization including individual level, group level and organizational level. Each of the three levels incorporates different key issues, forming a total of eight key issues (Martins, 2008): at organizational level: policy and procedures, benchmarking, risk analysis, and budget. At group level: management and trust, and at individual level: awareness and ethical conduct.

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. Each organization has its own information security culture similarly to every person having its own personality. 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). 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.

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 (Hinkle, 2007). Therefore, an approach that emphasizes an information security culture within the organization is required to make security as a part of employee's daily work routines. In order to develop a successful information security culture within an organization, it is important to understand both technical and non-technical aspects of information security (Rotvold, 2008).

2.3. Information Security Awareness

One thing worth mentioning here is the fact that security awareness training is very important tool to create as well as sustain information security culture in an organization. The level of security awareness, sensitivity, and reaction of people for security threats differ from culture to culture (Martins and Eloff , 2006). Information security awareness is important part of information security management. Information security awareness, a specific form of information security control, helps secure information assets by informing people about information security risks and controls in a general sense, and providing more specific information and guidance where necessary, emphasizing management's support for, and commitment to, information security, promulgating the organization's information security policies, standards, procedures and guidelines, and externally imposed laws, rules and regulations and motivating people to behave in a more security-conscious manner, for example taking security risks into account in business decision making (Rotvold, 2008).

Deloitte (2005), states "All parties with a need to know, including, but not limited to, information owners and information security practitioners, should have access to available principles, standards, conventions, or mechanisms for the security of information and information systems, and should be informed of applicable threats to the security of information. Awareness of information security principles, standards, conventions, and mechanisms enhances and enables controls and can help to mitigate threats. Awareness of threats and their significance also increases user acceptance of controls". In other words, without user awareness of the necessity for particular controls, the users can pose a risk to information by ignoring, bypassing, or overcoming existing control mechanisms.

2.3. Information Security Awareness

One thing worth mentioning here is the fact that security awareness training is very important tool to create as well as sustain information security culture in an organization. The level of security awareness, sensitivity, and reaction of people for security threats differ from culture to culture (Martins and Eloff , 2006). Information security awareness is important part of information security management. Information security awareness, a specific form of information security control, helps secure information assets by informing people about information security risks and controls in a general sense, and providing more specific information and guidance where necessary, emphasizing management's support for, and commitment to, information security, promulgating the organization's information security policies, standards, procedures and guidelines, and externally imposed laws, rules and regulations and motivating people to behave in a more security-conscious manner, for example taking security risks into account in business decision making (Rotvold, 2008).

Deloitte (2005), states "All parties with a need to know, including, but not limited to, information owners and information security practitioners, should have access to available principles, standards, conventions, or mechanisms for the security of information and information systems, and should be informed of applicable threats to the security of information. Awareness of information security principles, standards, conventions, and mechanisms enhances and enables controls and can help to mitigate threats. Awareness of threats and their significance also increases user acceptance of controls". In other words, without user awareness of the necessity for particular controls, the users can pose a risk to information by ignoring, bypassing, or overcoming existing control mechanisms.

The above study also found that about 45% of global organizations do not sensitive their employees in respect of possible information security threats and this lack of information security awareness could well lead to compromised information within the organization. Mitchell, Marcella, and Baxter (1999) found that information security awareness was concentrated around the information technology department and did not extend to information technology users. There can be major problems if organizations do not realize the importance of information security awareness amongst users (Von Solms, 2004).

It has long been generally accepted that authorized users and employees pose the greatest security threat to an organization and that raising and maintaining the awareness level of those people is a crucial part of an effective information security strategy (Ernst and Young, 2002). An effective information security program should include security awareness training to inform personnel (including managers and other users of information systems that support the operations and assets of the organization) about the information security risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce information security risks.

The objective of security awareness program is to ensure all relevant individuals understand the key elements of information security and why it is needed, and understands their personal information security responsibilities. Specific activities should be performed to promote security awareness (the extent to which staff understand the importance of information security, the level of security required by the organization and their individual security responsibilities – and act accordingly) across the enterprise. Staff should be provided with guidance to help them understand the meaning of information security (i.e. the protection of

the confidentiality, integrity and availability of information), the importance of complying with information security policy and applying associated standards/procedures, and their personal responsibilities for information security (Rotvold, 2008).

Organizations that do not have a security awareness program need to look seriously at beginning a security awareness program to strengthen their security defense system and protect their information resources. Technology alone is not a comprehensive solution. Involving top management and getting their support is essential in building a strong security awareness program that employees will take seriously. If management commitment is increased, and the security awareness goals and message are communicated and communicated often, progress and improvement can be made in creating a security culture (Rotvold, 2008).

2.4. Factors that Influence Information Security Culture and Practices

This section examines the information security management factors and a cultural issue that may influence information security culture and practices. The literature drawn for this analysis has largely been sourced from work investigating information security culture and practices in developed countries such as the USA, the UK and Australia and we can use this analysis as a guideline for identifying factors that influences the creation of strong information security culture and practices. According to these investigations, the different factors and issues which influence information security culture and practices are classified in to: corporate citizenship, legal regulatory environment, corporate governance and Cultural factors which are discussed below.

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 ideally committed to their security mission. Information security awareness is 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, 1999). Hinde, (2002) suggests that the absence of awareness programs indicate a critical gap in effective security implementation. Security training and awareness programs are therefore a fundamental component of effective information security strategy. Security awareness and training can help organizations to minimize some of the damage caused by misused or misinterpreted application procedures (Straub, 1990).

Legal and regulatory environment is another important factor that influences information security culture and practices. This issue is concerned with the concept of information security policy and information security management standardization and best practices. International best practices for information security management are based on the combined experiences of several influential international companies concerning the way in which they manage their information security (Von Solms, 2001). Information security management standards are used to establish and maintain a secure environment for information. Information security management standards can give customers and business partners the assurance that services are provided in a secure way, and can increase customer confidence in their business as well as businesses confidence in the organization's business systems (Eloff and Von Solms, 2000).

The major component of legal and regulatory environment is information security policies. The primary objective of information security policy is to define the users' rights and responsibilities in terms of information within an organization (Hong, et al., 2006). Effective information security policies will help users understand what is acceptable and responsible behavior in information resources and will assist in establishing a safe information environment (Höne and Eloff, 2002). Information security policy is an essential part of security practices within organizations and could substantially influence on their organizational security. As Higgins (1999) notes, without a policy, security practices will be developed without clear demarcation of objectives and responsibilities, and will face major difficulties when implementing information security management system effectively in their organizations' infrastructures.

Most employees were unaware of the information security policy and what is expected of them to aid in securing the organization's information assets. This implies that the information security policy needs to be created, reviewed and incorporated into the working environment for the requirements to become part of the everyday activities of the employees. Employees need guidance in what behaviors is acceptable and what is not. The organization needs to implement procedures such as awareness sessions and training programs to support and communicate the information security policy from the organizational level. This will encourage employees to adhere to the information security policy, thereby instilling the correct behavior, which is needed for an acceptable information security culture (Martins and Eloff, 2006).

Organizations cannot achieve effective information security management system without the establishment, implementation, and maintenance of an information security policy (Hong, et al., 2003). The formulation and utilization of information security policy can enhance the effectiveness of information security management system (Fulford, 2003). However, even though some organizations have established information security policy, it does not ensure that employees will necessarily obey these policies. As a result, policy enforcement is necessary and essential for the organizations' success (Von Solms, et al, 2004).

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 studies 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.

The British Standards Institute (1999) emphasizes that visible commitment from management and a good understanding of security requirements is key factors affecting the success of the information security management. Support from executive management not only influences uptake of affected information security policy but is also necessary for promoting appropriate information security management activities including information security awareness and training programs, information security compliance, information security risk analysis, and information security management standardization. A lack of

commitment from senior management is a major issue that organizations face in their information security management operations (Von Solms, 1996) and may often be found in organizations having difficulties managing their information security. Information security compliance processes help organizations compare their actual information security operations with international information security management standards (Karabacak and Sogukpinar, 2006).

2.5. Challenges to information security culture

While most research have concentrated on international organizations in developed countries such as the USA, the UK, Australia, and Europe, little is known about the particularities of information security management in the developing countries. Globally information security best practices and trends are similar. When it comes to applying these best practice approaches to specific applications, however, localized variables and limitations need to be emphasized. This is the case when we consider the application of generic best practices to a specific country, particularly a country which may be considered as still developing technologically. The following points discuses the major points of difference.

Studies have 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). The importance of non-technical issues related to security management, however, is de-emphasized in many studies which tend to be quantitative by nature (Siponen and Oinas-Kukkonen, 2007). Particularly, with respect to developing countries, there is a resulting lack of attention in the open literature on factors such as the national and organizational culture, environment and level of awareness and how these factors relate to generic attitudes towards information security and its management. Security

has always been identified as one of an information system's important components. Contemporary information assurance management recognizes the imperative to include people and processes, as well as the more traditional technology security issues, in ensuring the quality of information in all modern organizations. To a large extent technological solutions for the majority of security issues have been previously developed. There are however still many application challenges, the people and processes components of information assurance management.

Legislation and laws should provide the basis for ensuring an adequate level of compliance to international regulations and laws as well as giving internal direction. The increased demand from society for the protection of privacy and personal data has led several countries to develop their own privacy laws, for example the Australian Privacy Act (AU, 1988) and the European Data Protection Directive (EUDP, 1995). Many developing countries have yet to consider adopting adequate legislation related to information security management, laws that criminalize cyber attacks and enable police to adequately investigate and prosecute such activities (UN, 2005). In addition, many do not have privacy or network security laws or regulations which could be used to take action against the misuse of information communication technology resources (Aljifri et al., 2003). This implies that many developing countries are not only limited in taking action against intruders targeting their information assets but also against intruders who might use their country's information network as a base to perform illegal activities globally.

Organizations can avoid losses related to computer breaches if more commitment and deterrence is given (Dhillon, 1999). Key to the success of the commitment planning process is that commitments are defined and measured in objective terms (Siponen, 2000). The effective development of the information security program is carried out on the basis of the contractual attitudes between the organization stakeholders (senior management, technical staff, users and third parties). In many developing countries there is still a need for more effort regarding developing Information Communication Technology policies (UN, 2005). For example, the absence of Information Communication Technology security policy and its enforcement has been viewed as a major cause of fragmentation in the rules, procedures and practices leading to inadequate information security programs (Bakari et al.). This allows us to propose that the likelihood may be greater in developing countries, where in general policies are not in place, that a lower level of organizational commitment prevails than in developed countries.

Skilled staff and adequate continuous training programs have been recognized as an important factor for the success of information security programs (Ho, 2002). Generally in developing countries, even when the need for security is recognized, management decisions are limited by scarcity of budget and technical personnel (Rao, 2002). Another focal point is that senior managers and users may not be aware of the security challenges. Each one of them holds certain assumptions, attitudes and values towards the information system implementation and use processes. This can lead to a mismatch of priorities between the organization and its staff as end users. As a consequence, the lack of senior managers' awareness might hinder their willingness to commit sufficient resources. On the other hand,

there are the users who might misuse the system due to the absence of a proper awareness program (Bakiri, 2005).

In developing countries many organizations often face acute internal resistance when implementing new information and communications technology systems as employees may view this as a threat to their jobs. Besides individual resistance, organizations themselves are conservative inherently and oppose change (Salman, 2004). In terms of information security infrastructure, developing countries are also lack the necessary security technology structures (Aljifri et al., 2003).

3. Research Methodology

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, descriptive survey research method was used. To secure dependable information, both qualitative and quantitative methods were employed. Dawson (2006) suggested that there is no hard and fast rule to use the one and reject the other. Instead, prevailing trends favor the use of both designs in a single study. Dawson (2006) described that each data collection instrument has its own weakness and strengthens. Regardless of this, the same authors suggested that using each instrument accordingly as long as it is appropriate to the purpose, size and situation under which the research is conducted. Dawson (2006) also stated that the use of multiple data collection instruments as a rule because each reveals different aspects of empirical reality.

3.1. Study Site

This investigation was conducted in Hawassa Referral Hospital. This public hospital, which is the only referral hospital in SNNP Region, is found in Hawassa city. According to the data obtained from the medical director's office, the hospital provides medical services for more than 500 patients per day. The hospital provides general medical (emergency, general outpatient service like regular medical OPD, referral medical clinic, Leprosy, ART, VCT, in-patient), surgical (minor operation, regular OPD, surgical referral, minor orthopedic, surgical impatient), gynecology and obstetrics emergency (labor and delivery), pediatrics (in-patient services, emergency and OPD level), ophthalmology (out-patient, in-patient, internal ocular or lens alteration including cornea transplant), and so on. In addition to these service, the

hospital has been providing teaching in different departments (Medicine, Health officer, Nursing, Environmental health, laboratory and optometry).

3.2. Study Design

Cross-sectional survey was used as a study design in this investigation. This study design was used to gather all the necessary data from a population at a defined period of time. The investigator will collect all the necessary data and information from selected sample or section of the population at a defined period time.

3.3. Study Population

3.3.1. Population of the study

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 are primarily involved in health data gathering, processing and dissemination. According to the data obtained from Human Resource Information Office of the hospital in March 2010, there were 306 health care providers and 120 administrative and supportive staffs who are working in HRH. In addition, the data obtained from Hawassa University Medicine department indicates that there were 138 internship clinical and medical students. Thus, the total size of the target population of the study was 564.

3.3.2. Sampling Techniques and Procedure

With respect to the determination of the size of the sample, there is no one formula in the literature of the research. As a result, researchers use different formula to determine it. Nonetheless, in this study, the size of the sample was determined by using the formula which was proposed by Yemmane (1968). The rationale behind is that it considers the non-response rate and standard error. On top of this, it is highly recommended for conducting survey study. Accordingly, the size of the sample was determined as follows

$$n = \frac{N}{(N + 1) E^2} + c$$

Where n = the required total sample size, N = the total size of the population (N =564), E = maximum standard of error (E = 0.05) and C= contingency

$$\frac{564}{(564 + 1) (0.05)^2} + 10\%$$

$$n = \underline{\underline{350}}$$

To select respondents from the target population of the study, stratified sampling technique was employed. The reason behind is that the respondents do vary in their educational qualification, profession, exposure to health information in hospital, and so on. To say it differently, the target populations are heterogeneous. Hence, as shown in the table below, the respondents were taken proportional from each stratum.

Table 3.1- Sampling Frame

Strata	Population	Sample
Health care providers	306	190
Administrative staff	120	74
Medical students	138	86
Total	**564**	**350**

To select respondents from each stratum, simple random sampling techniques (lottery method) were used. The logic behind 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.

3.4. Data Collection Tools

In order to get enough information from respondents, a combination of data collection methods were used. To this end, both qualitative and quantitative research approach were found to be relevant in this study to gather data.

3.4.1. Quantitative Components

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 contains key information security culture issues such as information security policy, procedures, benchmarking, risk analysis, budget, management commitment, individual awareness and ethical conduct. In addition to this, its usefulness and practicality had already been tested in different studies in developing countries including South Africa. The information security culture questionnaire was translated in to 'Amharic' to make

questions brief and clear to respondents. The 'Amharic' version of the questionnaire was translated back to English to cross check and to make all the necessary correction. Both translations were made by English and Amharic instructors in Debub University. To make the data collection more effective, three IT professionals were selected as a data collector based on their work experience (having experience of data clerk). And then short term training was given for one day by the researcher so as to make the objective of the questionnaire clear and to clarify questions. On top of this, the researcher also closely assisted and supervised them during the data collection. The data collection was conducted with the 'Amharic' version of the questionnaire for the entire respondent.

3.4.2. Qualitative Components

Since this research focuses on the study of socio-cultural issues, it is 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-depth interview was used only for medical director, medical record department head and human resource record department head because it will not be possible to administer in-depth interview for medical staff due to workload and short time schedule on duty.

According to Beryman et al. (2007, pp. 322-323), where the respondents and researchers have not been in contact before, the first few minutes of conversation will have a significant impact on the interview's outcome. The researchers need to explain the study to participants to establish credibility and gain interviewee's confidence. The interviews therefore were conducted by using the interview guidelines commencing with an introduction of interviewer, research title, the objective of the research and estimated

interview length. The presentation was kept clear and brief in order to reduce anxieties and make interviewees more relaxed and open.

Interviews were arranged in the afternoon when interviewee had free time and were not in a hurry of work. Tape recorder was not used because of the refusal of the key informants to be recorded. In addition to this, the data gathered through in-depth interview was supplemented by reviewing such documents as strategic plan, financial report and other necessary documents.

3.5. Data Processing and Analysis

The main purpose of this investigation is to assess the information security culture of public hospitals in SNNPR particularly the case of Hawassa Referral Hospital. To do this, different statistical method were used for analyzing the data. Obtained responses from the questionnaires were systematically coded. The quantitative data was integrated, summarized and analyzed by using SPSS version 15.0. The qualitative data was analyzed manually. Responses of each key informant were initially categorized based on thematic issues addressed; then similar issues were merged to the selected thematic area. Finally, the responses of the in-depth interview were summarized by five thematic issues. In addition to this, some of the ideas of the key informants were quoted.

3.6. Data Quality Management

Various efforts were conducted to assure the quality of data. Personal supervision was employed to ensure the quality of the data collected during the process of data collection. Before the information security culture questionnaire and the in-depth interview questions were used on the study site, they were pre-tested on randomly selected 20 health care providers and medical students in Black Lion Specialized Hospital to allow the researcher to understand the anticipated reaction of the larger group and to revise or restructure questions where necessary.

3.7. Ethical Consideration

Ethical clearance were initially obtained from the Research Ethics Committee at the faculty of Informatics and got approval from the joint academic commission of Faculty of Informatics and School of Public Health in Addis Ababa University. In addition to this, ethical clearance was also obtained from Ethical Review Board of Hawassa University Referral Hospital. Oral consent was sought before administering questionnaire and conducting interview from each selected participants to conform their willingness and those who were not willing were given the right to do so. Before starting the in-depth interview, the investigator communicated the participants about the objective and the significance of the study to get the consent of the respondents and to enhance the response rate.

3.8. Dissemination Plan

This thesis report was submitted and presented to the School of Public Health and to the department of Information Science of AAU. The finding of the research was also shared and discussed with Hawassa Referral Hospital management committee. This thesis report will also be submitted to Federal Ministry of Health, SNNP Regional Health Bureau and Federal Ministry of Education.

4. Data Presentation and Analysis

4.1 Introduction

The attitude, belief and actions of employees towards information must be acceptable and needs to be part of everyday life in 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. In addition to this, it is always necessary for organization to assess their information protections activities and controlling mechanism to ensure that their activities and efforts are producing an acceptable level of information security culture in the organization. The main aim of this research is to assess the attitude and knowledge of Hawassa Referral Hospital health care providers, administrative employees and medical students towards information security.

Different data collection tools have been used in this research to assess the existing information security culture in the hospital. The perception, attitude, opinions and action of health care providers, medical students and other administrative employees regarding information security culture was assessed by using questionnaire, in-depth interview and document analysis.

The first section of the questionnaire contains knowledge questions that are analyzed separately from other information security culture statements. The knowledge questions can be used to obtain information pertaining to the current knowledge of employees that could result in specific behavior (da Veiga, Martins & Eloff, 2007). The second section is the

information security culture statements which asses the perception of employee about the above eight different issues of information security culture.

All study subjects who participated in the questionnaire were asked questions about the meaning of information security and its relation with their daily job, information security policy and procedure and the assistance of the management towards the implementation of information security in the hospital. Added to this, in-depth interviews were also conducted with medical record department head, human resource processing team leader and with medical director of the hospital in order to get detail information about the issue under study. Furthermore, to get all the necessary and genuine information which cannot be directly collected from questionnaires and in-depth interview, document analysis was used in different organization documents including annual organizational plan and report, strategic plan and different policies to triangulate the information. The last phase of this study address the discussion, conclusions and recommendation based on the data obtained from the study.

4.2 Quantitative Study

4.2.1. Demographic Characteristics of Respondents

A total of 311 respondents were included for the final analysis of the quantitative study making the overall response rate of 88.9%. During the data collection, it was difficult to get completed questionnaires on time from respondents mainly due to workload 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.

Table 4.1: Socio-demographic characteristics of respondents in HRH, March-April, 2010.

Characteristics	N=311 Frequency	%
SEX		
Male	201	64.6
Female	110	35.4
TYPES OF RESPONDENTS		
Medical students	86	27.7
Health care providers	164	52.7
Administrative staff	61	19.6
AGE GROUP		
20-29	137	44.1
30-39	110	35.4
40-49	40	12.8
+50	24	7.7
SERVICE YEAR FOR HCPs	**N=164**	
<=5 years	108	65.9
6 to 10 years	36	22.0
>10 years	20	12.1
EDUCATION QUALIFICATION (HCP)	**N=164**	
Diploma	64	39.0
First Degree	80	48.8
Above	20	12.2
PROFESSIONAL CATEGORY (HCP)	**N=164**	
Specialist physician	58	35.4
Clinical nurse	64	39.0
Pharmacist	9	5.5
Medical laboratory	11	6.7
Others	21	12.8
YEAR OF STUDY	**N=86**	
Internship	32	37.2
Final year clinical nurses	34	39.5
Final year midwives	20	23.3

As can be seen from the above table, 164(52.4%) of 311 respondents were health care providers, 86(27.7%) of the respondents were medical students who are providing health care service at different wards in the hospital and 61(19.6%) of the respondents were administrative and supportive staffs during the study period. From the total of 311 respondents, 201(64.6%) of the respondents were males and the rest 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(37.2%) were internship medical students, 34 (39.5%) were clinical year medical students, while the remaining 20(23.3%) were midwives students.

Among the total respondents of health care providers 64(39.0%) were diploma holders, 80(21%) were first degree holders and the remaining of the respondents were master and above holders. As far as their profession is concerned, 58(35.4%) of the respondents were specialist physician, 64(39.0%) were nurses, 9(5.5%) of the respondents were pharmacist, 11(6.7) of the respondents were medical laboratory and 21(12.8%) were other professionals. Among those health care providers who participated in this study, 108(68%) of the respondents have less than five years of the experience, 36(22.0%) of the respondents have between five and ten years experience and the remaining respondents had above ten years of experience.

The following data analysis is based on the dimensions in which a large number of interrelated questions were combined together to make the data analysis more easy. These dimensions were identified by the study conducted by Brewerton and Millward (2001)

4.2.2. Knowledge to Information Security

The information security culture questionnaire is divided in to three sections (Martins, 2002): (1) Information security culture statements, (2) Knowledge questions and (3) biographical questions. The first phase of this quantitative analysis involves determining how much knowledge employee have about information security and whether a low information security culture results from an educational problem or from perceptual concerns.

	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%)
5	The hospital has a written information security policy.	15 (8.0%)	286 (92.0%)

Table 4.2 summarizes the responses of research participants on five knowledge questions. Firstly, 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 5.2 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. In addition to this, the above table also shows that overwhelming majority of respondents that constitute 286 (92.0%) of 311 do not know if the organization has a written information security policy while the remaining 15 (8%) of 311 respondents know the existence of a written information security policy in the hospital.

In general, as it can be observed from the above table, majority of health care providers, administrative and supportive staff and medical students do not know what the term information security implies. In addition to this, majority of the respondents also do not know the existence of information security policy or plan in the hospital. From this, it is not difficult to see that the absence of knowledge about information security may be caused by absence of information security awareness program in the hospital. It is also possible to infer that respondents' lack of knowledge about information security policy or plan may be caused by the absence of information security policy or plan in the hospital.

4.2.3. Management of Information Security

This dimension includes the applicability of information security policy, the understanding of threats to information assets, a willingness to change working practices to ensure the security of information assets, 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%)	111 (35.7%)
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 (34.4%)	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 4.3 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. Regarding the importance of allocating specific budget for the operation of information security, 209(70.4%) 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%) of 311 respondents 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. This would indicate that majority of the respondents are ready to change their working practice in order to ensure the security of information. In other word, 83(26.7%) of 311 respondents replied strongly disagree or disagree to the proposition that would indicate the existence of significant number of employee who are not ready to change their working practice for the security of information.

Regarding the third item, 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 i.e. I have a responsibility towards information security in the hospital. The rest of respondents said agree or strongly agree to the above statement. From this explanation, it is equally natural to say that most of the respondents reported that they are not responsible for information security in the hospital.

Concerning the availability of information to employee outside of the hospital, majority of the respondents that constitutes 204(66.7%) 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 statement respectively. This shows that most respondents believe information about the hospital should be available for employee in the organization.

The responses in the above table indicate that the hospital need to work more on increasing the awareness level of employee to increase their responsibility towards information security in the hospital. The entire employee in the hospital need to participate in the training program because securing information should get the attention of all employees and health care providers in the hospital. It should not be left to few employee i.e. only to health care providers. In addition to this, the hospital also needs to communicate procedures that are implemented in the hospital to stress what is expected of all employees in securing information in the hospital.

4.2.4. Communication

The information security cultural statements included in this dimension focus on aspects such as the explanation and communication of information security policy, informing employee in a timely manner how information security changes will affect them 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%)

Table 4.4 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 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. This may indicate that information security is not viewed as an important issue in the hospital.

Regarding statement 2 in Table 5.4, majority of the respondents 221 (71.0%) of 311 said strongly disagree or disagree. The rest of respondents which constitute 79(25.4%) of 311 and 11(3.6 %) of 311 respondents responded unsure and agree or strongly agree to the statement respectively. Accordingly, it is fair to say that majority of the respondent do not believe the management has communicated information security information to all job levels. The management need to conduct open dialog and discussion with employees concerning information security, arrange awareness creation training program and allocate enough budget for preparing security posters, gowns and pens with security messages to communicate information security information for employees in the hospital.

4.2.5. 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 asset.

	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 (37.0%)	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 4.5 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 above finding indicates that majority of the respondents believe in the importance of implementing information security.

The research finding, as shown in Table 5.5, also revealed that majority of the respondents i.e. 174 (56.0%) of 311 respondents strongly disagree or disagree to the information security culture statement i.e. management assists in the implementation of information security. On the other hand, 114(36.7%) of 311 respondents said unsure while 23(7.4%) of 311 respondents said agree or strongly agree. Concerning the perception of the management about the importance of information security, the majority of respondents that constitute 230 (73.7%) of 311 replied strongly disagree or disagree. Among the rest of respondents, 54(17.4%) of 311 replied unsure while 26(8.6%) of 311 respondents agree or strongly agree to the statement.

Research 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.

From the above responses, it can be learnt two things. First, majority of the health care providers, medical students and administrative staffs believe the importance of implementing information security in the hospital. Second, they also don't believe that management has assisted the implementation of information security in the hospital. The above table also showed that more than half percent of the respondents do not consider information security as technical or functional issue.

4.2.6. Performance Accountability

Performance accountability focuses on aspects such as adherence to information security policy by various business areas, whether action should be taken against people that do not adhere to the information security policy 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 4.6 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%) of 311 and 54(17.3%) of 311 respondents replied strongly disagree or disagree and strongly agree or agree respectively. In the above table it is also indicated that, majority of the respondents that constitute 214(68.9%) of 311 strongly disagree or disagree to the statement 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 to 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%) of 311 the respondents strongly disagree or disagree while 28(9%) of 311 remained unsure. On the other hand, 83(26.9%) of 311 respondents said agree or strongly agree to the statement. It can be said that most of the respondents do not held themselves accountable if they don't adhere to the information security policy.

5. Qualitative Study

5.1.Introduction

This research is interested in assessing the information security culture at public health hospitals in SNNPR, more specifically in Hawassa Referral Hospital. Assessment of information security culture involves looking at all the key issues described at the information security culture model which includes policy and procedures, benchmarking, risk analysis, budget, management, trust, awareness and ethical conduct.

To this end, both qualitative and qualitative research approach were found to be relevant in this study to gather data. In the quantitative approach, the questionnaire of Martins (2008) was used to assess the information security culture of the hospital. This instrument has incorporated the eight key issues for assessing information security culture. Besides, since this study focuses on the study of socio cultural issues, it is equally important to use the qualitative approach which is concerned with developing explanations of social and cultural phenomenon (Miles and Huberman, 1994).

5.2.Description of the respondents

A total of three key informants were involved in the in-depth interview drawn from senior management and medical and human resource record department. One of the key informants was clinical service and practical training director of the hospital. The other two are head for medical record department and leader for human resource processing team. The clinical service and practical training director was working as a physician and as an instructor in the medical department. The human resource processing team leader was working for more than five years in the human resource processing department. The head for medical record

department was working for the last three years as data clerk and as a head in the department. Below are some of summarized thematic issues of the discussion with the key informants during the in-depth interview.

- Knowledge of information security.
- The existence of physical or any other mechanism for the protection of information assets in the hospital
- Factors or issues that hindered effective implementation of information security culture in the hospital.
- The commitment of the management towards the implementation of information security.
- Measures that should be taken to improve the information security culture in the hospital.

5.3. The existing information security situation in the hospital.

Medical records should be safeguarded against unauthorized use, modification and disclosure. They should be stored in a secure area, and there should be detail policies regarding confidentiality and the release of patient information. It is best to have a written policies relating to the use of patient information and staffs must be familiar with these policies. The result obtained from the in-depth interview with the key informants indicated that all the key informants reported that information in the hospital is not adequately protected both physically and electronically. One of the key informants explained the existing situation in the following plain language:

"Patient records are missing, sometimes patient records are not properly returned to medical record room and medical records are also used for educating nurses with less care for patient identity and etc."

It was also reported by one of the key informants that there is lack of physical or electronic mechanism to protect both medical and human resource information. For instance, there is no well written and documented information security policy in the hospital. According to the key informant, medical records are left in the table or office area where anyone can access or see it. In addition to this, medical records are not properly handled in medical record room and authorized access to records is not maximal.

5.4.Knowledge to information security

In the quantitative study, it was indicated that 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 information security implies. It is easy to see that more than half percent of the respondents do not know what the term information security implies to them. All of the key informants participated in this interview had lack of awareness about information security. All of them explained information security in relation to systematic record keeping. One of the key informant explained information security as

"It is the systematic processes of keeping records and protecting those records from external harm or danger."

According to another key informant, information security is the protection of information from external harm or danger.

5.5. Challenges to information security in the hospital.

All of the key informants believed that information in the hospital is not adequately protected. They believed that it is important to implement and use information security in the hospital. According to one of the key informants, some of the factors or issues that hindered effective implementation of information security in the hospital are:

"Lack of automated system and ICT infrastructure, absence of organized and systematic record keeping system, the existence of large amount of patient records, lack of skilled man power, lack of resources including skilled man power and absence of a clear policy that govern the information use of the hospital"

Another key informant also reported that the lack of awareness among health care providers and other staffs about the confidentiality of patient information and the existence of large amount of medical records in medical record room are the two main reasons for the absence of effective information security in the hospital.

5.6 Information protection efforts in the hospital.

Key informants participated in this interview reported that the organization has implemented certain mechanism to protect information resources in the hospital. Some of the mechanisms implemented in the hospital are: the human resource records are translated in to electronic form in addition to the manual record and access to medical records for researcher is permitted through letter from the medical director. However, all of the key informants believed that the mechanisms implemented are not adequate enough to protect medical and

human resource information from harm. One of the key informants expressed his view about the information protection efforts of the hospital as follows:

"Information protection efforts are not adequate in the hospital. However, some mechanisms have been implemented recently. Request for medical records from medical record room by any health care provider or researcher is permitted through letter."

5.7.Factors or issues to improve the situation.

The key informants participated in the interview believed that management need to understand issues or factors that will improve the situations in the hospital. All the key informants reported that information security is not considered as a challenging issue in the hospital because of lack of awareness to information security. They also reported that it is not considered important like any other function in the hospital. One of the key informant explained information security situation in the hospital as a "worst" compared to what he saw in other hospitals. As a result, he listed the following points to improve the situation:

"Improving and using ICT infrastructure, using an automated record system and formulating laws, regulation or policy."

The medical record department head also reported that attention should be given for training to increase the awareness level of health care providers and other staffs in the hospital.

6. Discussion

The attitude, belief and actions of employees towards information must be acceptable and needs to be part of everyday life in the organization. Many researchers proposed a technological approach to solve most of the problems related to information security. However, it has been recognized that non-technical issues are as important as technical issues in safeguarding an organization information assets. The main aim of this research was to asses the knowledge and attitude of health care providers and administrative staff in order to facilitate the implementation and adoption of information security culture in the hospital. This study also recommends measures for improving information security culture and practices in the hospital.

Literature in the area of information security showed that research in the area of information security culture is still in the early stage of development, especially in developing countries. Most of the investigation in the issue of information security culture and practice were done in developed countries such as USA, UK and Australia. Only few researches were done in developing countries such as South Africa and United Arab Emirate. Thus, although its practical implication takes the lion's share, this research contributes to the body of knowledge in the area of information security in general and to information security culture in particular.

Traditionally, most of the researchers believed technological approach to address the majority of information security issues. However, in order to bring adequate information security culture and practice, it needs a socio-technical approach in which we involve people,

process and technology. In other words, both technical and non-technical issues should be considered to bring effective information security culture in the hospital.

The results obtained from both quantitative and qualitative study impressively showed major important findings about information security in Hawassa Referral Hospital. 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%) of 311 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. This data impressively show that only 15.1% of the respondents know information security related to their job.

According to Hinde (2002), the absence of security awareness indicates a critical gap in effective security implementation. In general, form the above three results, it can be deduced that there is lack of awareness about information security among respondents. It was also showed that, overwhelming majority of the respondents that constitute 244 (78.5 %) of 311 strongly disagree or disagree to the information security statement i.e. I am trained in the information security controls I am supposed to use. In 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 of 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 is lack of awareness among key informants about information security. In similar manner, it is 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 few of the more common reasons given for security awareness training not being conducted.

The study indicated that majority of the respondents of this study have never received an information security awareness training. As a result, majority of the health care providers and other staffs need extra-information security awareness training and education. According to Dhillon (1999), increasing the awareness of security issue 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. In addition to this, health care organization and other concerned bodies can also implement and incorporate a course with a special information security education in health curriculum to bring adequate level of information security awareness.

Even though education and in-service awareness training are the basis for creating security conscious employee, they do not guarantee security conform behavior in the daily work environment. Awareness measures outside of the class or training session such as security posters, mouse pads, pen and gown with security slogan help to make security topics omnipresent. In addition to this, the organization can communicate information security messages by using periodic discussions and dialog with members of the organization.

Organizations also need to realize the importance of information security training to all concerned employees in the hospital.

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 to the information security culture statement which indicates the assistance of the 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 study revealed that the highest level of respondents (92.8%) 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 e 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 will be developed without clear demarcation of objectives and responsibilities. Effective information security policies will 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 employees behavior in relation to information.

However, the establishment and implementation of information security policy do not ensure employees will necessary obey these policies (Von Solms, 2004). In this study, it was indicated that more than half percent (57.6%) of the respondents reported that they are unsure whether they are adhering to the organization information security policy or not. In similar manner, it was also indicated that 25.0% of the respondents strongly disagree or disagree to the above proposition. 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. The study conducted by Karabacak (2006) also indicated that organizations need to evaluate their information security compliance level. Organizations 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 results from employees failure to comply with security policies. As a result, policy enforcement is necessary and essential for the success of information security policy.

In this study, it was indicated that 71.1% of the respondents responded that management does not communicate information security information on a need to know basis to all job levels. Management need to communicate information security policies by using different media such as information security awareness training and by using open discussion or dialogue. In this study, 61.7% of the respondents indicated that they can not easily obtain a copy of information security policy. The organizations need to place a copy of the policy in a convenient place where anyone could easily access or read it.

The study also revealed that 83% of the respondents strongly agree or agree the importance of implementing and using information security in the hospital. All the key informants who participated in the in-depth interview also reported the importance of implementing information security in the hospital. From this, it is sound to infer that majority of the research participants believed the importance of implementing information security in the hospital. It was also showed in this study that 64% of the respondents are prepared to change their working practice in order to ensure the security of information. This result reveals the existence of willingness and preparation on the side of respondents to change their working practices to secure organization information assets.

7. Strength and Limitation of the Study

7.1.Strength of the Study

- Combination of both quantitative and qualitative study.
- Since it is the first study in the area of information security culture in health institution, it provides baseline information for further research in other parts of Ethiopia.
- It included health care providers, medical students and other administrative staff as a study subject.
- Discussion of the study result with senior managers in the hospital.
- It emphasized the role of non-technical issues in safeguarding the organization information resources.

7.2.Limitation of the Study

- Lack of similar and published studies in the area of information security culture especially in developing countries.
- Presence of incomplete questionnaires i.e. some questionnaires are not complete.
- High workload to health care providers and senior managers.
- Lack of motivation and commitment from some health care providers to participate in the study.

8. Conclusion

To develop appropriate information security policy and to advance the information security culture to an adequate level in health institutions, it is worth to assess the perception, attitude, belief and action of employees and internship medical students with regard to information security. Such kind of research in health institutions can serve as a spring-board for the appropriate interventions like information security awareness program and for the formulation of information security policy. The results of this study have important implications about the existing information security environment in the hospital. These are some of the major conclusions of this study

- The study indicated that majority of the health care providers and other administrative employees in the hospital do not know what the term information security implies.
- Majority of the respondents in the hospital has never received information security awareness training.
- More than half of the respondents participated in this research reported that management do not assist the implementation of information security issues in the hospital.
- Majority of the respondents participated in this study believed in the importance of implementing and using information security in the hospital.
- The study found that there is no information security policy about how the data is stored, proceeds, disseminated or used in the hospital.
- The result from in-depth interview indicated that information in the hospital is not adequately protected.

- More than half of the respondents reported that they are ready to change their working practice in order to ensure adequate protection to information assets.
- Majority of the respondents reported that they are unsure whether they are adhering to the information security policy of the hospital or not.
- Majority of the respondents who participated in this research reported that they do not know a function, a team or a person who is responsible for information security in the hospital.

9. Recommendations

Most researchers believe that bringing effective and acceptable information security culture is continuous processes which require long term commitment and sustainable efforts from employees and management. The hospital needs to formulate an information security policy and implement procedures such as awareness session and training programs to support and communicate information security policy. Management also needs to incorporate information security as one of the characteristics of the hospital and demonstrate its commitment and involvement in the processes of implementing it effectively. The following are some of the recommendations based on the result obtained

9.1.Short Term

- The hospital should implement information security awareness training program to bring information security conscious behaviors. All the concerned parties i.e. senior managers, health care providers and other administrative staff should participate in the training program.
- Senior managers in the hospital should support and commit enough resources for the operation of information security in the hospital. Increasing the participation and support of the management is a key issue to bring sustainable information security culture 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 guideline, rules or regulation that guides employees how to use information assets in the hospital.

- Assigning a specific person or team who can take full responsibility for information assets in the hospital.
- The hospital should implement awareness measures outside of the class or training room to help employees remember the lessons learnt. Using security posters in the office and office areas and using gowns and pens to transmit security messages helps the security topic omnipresent.

9.2.Long Term

- Formulating health information security policy by involving key stakeholders from the health sector.
- Incorporation of information security topics or courses in the curriculum of health. Because the researcher believes that education is one of the core means for creating security awareness.
- Federal Ministry of Health should incorporate information security as one core processes or function in the hospitals.
- Appropriate ICT infrastructure which provides technical protection for information assets should be implemented in order to improve the information protection efforts of the hospital.
- It is the position of the researcher that detail investigation should be carried out involving every employee by using the survey approach to understand the differences in the awareness between employees in different wards or department in the hospital.
- The researcher also recommends further studies in information security culture in Ethiopia to have detail insights about the issue in different hospitals.

10. References

1. *Aljifri, H. A., Pons, A. and Collins, D. (2003). Global e-commerce: a framework for understanding and overcoming the trust barrier. Information Management & Computer Security, 11 (3), 130-138.*
2. *AU.1988. Australia Privacy Act 1988. www.privacy.gov.au/act/index.html. (Accessed July 2007).*
3. *Bakari, J. K., Tarimo, C. N., Yngstrom, L. and Magnisson, C. (2005) State of ICT Security Management in the Institutions of Higher Learning in Developing Countries: Tanzania Case Study. Computers & Security Proceedings of the Fifth IEEE International Conference on Advanced Learning Technologies (ICALT 05).*
4. *Beryman, A. & Bell, E. (2007) Business Research Methods, 2nd Edition, Oxford University Press Inc. New York.*
5. *Brewton, P. & Millward, L. 2001. Organizational Research Methods. London: Sage.*
6. *British Standards Institute. (1999). Information Security Management-BS 7799-1:1999. London: BSI.*
7. *Chang, S., E., Lin, C. (2007). Exploring organizational culture for information security management. Industrial Management & Data Systems, 107(3), 438-458.*
8. *Chen, C., C., Medlin, D., B. (2008). A cross-cultural investigation of situational information security awareness programs. Information Management & Computer Security, 16(4), pp. 360-376.*
9. *Dawn C. and Andrew M. (2007). Common Sense Guide to Prevention and Detection of Insider Threats, Carnegie Mellon University, USA, 3rd Edition at http://www.cert.org/insider_threat/study.html, accessed on June, 2007.*
10. *Da Veiga, A., Martins, N., & Eloff, J.H.P. (2007). Information security culture – validation of an assessment instrument. Southern African Business Review, 11(1), 147-166.*
11. *Deloitte, T. (2005). Global security survey, at http://www.deloitte.com/dtt/cda/doc/content.*
12. *Dhillon, G. (1999). Managing and controlling computer misuse. Information Management & Computer Security, 7 (4), 171-175.*

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

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

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

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

17. EUDP. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281, 31-50.

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

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

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

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

22. Hinde, S. (2002). Security survey spring crop. Computer & Security, 21(4), 310-321. Hofstede, G. (1984). Culture's Consequences: International Differences in Work Related Values. Beverly Hills: Sage Publications.

23. Ho, A. (2002). Reinventing local governments and the e-government initiative. Public Administration Review, 62 (4), 434-444.

24. Hinkle, P. (2007). "Mitigating IT Risks with Security Education and Training; Information Systems Security;" at http://www.infosectoday.com/Articles/Mitigating_ IT_Risks.htm viewed on September 10, 2009.

25. Hinson, G. (2009). The true value of information security awareness; Notice Board; at http://www.noticebored.com/html/why_awareness_.html viewed on September 28, 2009.

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

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

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

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

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

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

32. Martins, A. (2002). 'Information security culture', MCom dissertation, Rand Afrikaans University, Johannesburg.

33. Martins, A. and Eloff, J. (2006). Assessing Information Security Culture, Rand Afrikaans University, Johannesburg, South Africa.

34. Martins, E.C. 2000. 'Die invloed van organisasiekultuur op kreatiwiteit en innovasie in 'n universiteitbiblioteek', MCom dissertation, University of South Africa, Pretoria.

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

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

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

38. Peltier, R. (2002). Information Security Policies, Procedures, and Standards: guidelines for effective information security management. Boca Raton, FL: Auerbach publications.

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

40. Rao, M.2002. How real is the internet market on developing countries? www.isoc.org/oti/articles/0401/rao.html (Accessed July 2007)

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

42. Rühli, E. (1991). Unternehmungskultur - Konzepte und Methoden. In: E. Rühli and A. Keller, Eds. Kulturmanagement in schweizerischen Industrieunternehmungen. Bern und Stuttgart, Paul Haupt Verlag: 11-49.

43. Salman, A. (2004). Elusive challenges of e-change management in developing countries. Business Process Management Journal, 10 (2), 140-157.

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

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

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

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

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

49. Siponen, M. T. and Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. SIGMIS Database, 38 (1), 60-80.

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

51. Ulich, E. (2001). Arbeitspsychologie. Zürich, vdf, Hochschulverlag a der ETH Zürich.

52. UN. (2005). Information Economy Report, at http://www.unctad.org/ecommerce/

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

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

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

56. Weise, Joel and Martin, Charles R (2001). Sample Data Security Policy and Guidelines Template, Sun Blueprints Online, December 2001, at http://www.sun.com/blueprints/tools/samp_sec_pol.pdf.

57. Yeats, D. (1996). Project management for information systems. Second edition. London: Pitman Publishing.

Annexes

Annex 1. English questionnaire.

ADDIS ABABA UNIVERSITY
FACULTY OF INFORMATICS
HEALTH INFORMATICS PROGRAM

I am Temesgen Gebrasilase, a post-graduate student in Health Informatics at Addis Ababa University, Faculty of Informatics. Currently I am doing my masters thesis entitled **"Assessment of Information Security Culture in Public Hospitals in SNNPR: The case of Hawassa Referral Hospital".**

The objective of this questionnaire is to collect data from health care providers, administrative staff and from medical students on their knowledge, attitude and perception towards information security. In line with this, it also helps to identify and asses issues that facilitate the implementation of information security culture and practices in public hospital. It will take about 30 minute to fill the questioner. You are selected to participate in this study just by chance. The information you provide us is extremely important and invaluable, as it will help the government and private institution involved in providing health service around the country.

I would like to assure you that the information that you provide me is completely confidential and will be used only for the research purpose. You have full right to refuse to take part or to stop filling the questioner at any time. But the information that you provide me is quite useful to achieve the objective of the study and to contribute for assessing the existing information security culture of health institution.

Considering the information you get from the general information above, I would be thankful if you spend some time to answer questions related to the issues.

Name of data collector_____
Signature_____
Date_____

Name of Supervisor_____
Signature_____
Date_____

ADDIS ABABA UNIVERSITY
FACULTY OF INFORMATICS
HEALTH INFORMATICS PROGRAM

A questionnaire to asses the knowledge, attitude and belief of health care providers and other administrative staffs on information security culture in Hawassa Referral Hospital.

PART I: - DEMOGRAPHIC CHARACTERSTICS

Instruction: In this section, please fill your personal information that exactly fits your status on the space provided.

NO	STATEMENT	ANSWER
1	What is your sex?	
2	What is your age?	
3	Student/Heath care providers/administrative staff	
4	Field of graduation(*this is only for heath care providers and administrative staff*)	
5	Educational qualification (*this is only for heath care providers and administrative staff*)	
6	Field of study (*This is only for medical students*)	
7	Year of study (*This is only for medical students*)	
8	Year of experience in the hospital? (*this is only for heath care providers and administrative staff*)	

PART II. KNOWEDGE QUESTIONS

Instruction: For the following questions please put "✓" symbol in front of the space provided in each knowledge questions.

NO	STATEMENT	YES	NO
1	I know what the term information security implies.		
2	I am aware of information security related to my job.		
3	I know a person or a team responsible for information security in the hospital.		
4	The hospital has a written information security policy.		
5	The hospital has an information security plan.		

PART II. INFORMATION SECURITY CULTURE STATEMENTS

	Statements	Strong Disagree	Disagree	Unsure	Agree	Strongly Agree
1	It is important to determine the hospital's information security needs.					
2	Information security should be regarded as a functional issue.					
3	Information security should be regarded as a technical issue					
4	I think it is important to implement information security in the hospital.					
5	I am trained in the information security controls I am supposed to use.					
6	I have a responsibility towards information security in the hospital.					
7	Management assists in the implementation of information security issues.					
8	Management perceives information security as important.					
9	I adhere to the hospital's information security policy.					
10	The hospital ensures that I adhere to the information security policy.					

11	All information about the hospital should be available for non-employee.					
12	All information about the hospital should be available for employee.					
13	I should be held accountable for my actions if I don't adhere to the information security policy.					
14	Procedures are implemented to support the information security policy.					
15	I can easily obtain a copy of information security policy.					
16	It is important to budget annually for information security spending/coast.					
17	I am prepared to change my working practices in order to ensure security of information.					
18	Management perceives information security as important.					
19	Management communicates information security information on a need to know basis to all job levels.					

Thank you for your patience to complete this questionnaire!!

Annex 2. Amharic questionnaire.

አዲስ አበባ ዩኒቨርስቲ

የድህረ ምረቃ ትምህርት ክፍል

የሄልዝ ኢንፎርማቲክስ ፕሮግራም::

የዚህ መጠይቅ ዋና ዓለማ በሀዋሳ ሪፈራል ሆስፒታል በሚሰሩ የጤና ባለሞያዎች፣ የአስተዳደር ሠራተኞችና በሆስፒታሉ ጤና ሳይንስና ሜዲካል ኮሌጅ በተግባር ልምምድ ላይ ባሉ ተማሪዎች ስለ መረጃ ደህንነት አያያዝና አጠባበቅ ያላቸውን ግንዛቤ፣ እምነት፣ አመለካከትና ዕውቀትና ተግባር ለማወቅ ነው:: ስለሆነም በሆስፒታሉ የሚሰሩ የጤና ባለሞያዎች፣ የአስተዳደር ሠራተኞችና በተግባር ልምምድ ላይ ያሉ ተማሪዎች የሚሰጡት እውነተኛ መልስ የጥናቱን ዓላማ ከማሳካት አልፎ በሀገራችን ባሉ የጤና ማእከላትና ሆስፒታሎች ያለውን የመረጃ ደህንነት አያያዝና አጠባበቅ ባህል ለማሻሻል ይረዳል:: ስለዚህ ውድ የጥናቱ ተሳታፊዎች ይህን ከግንዛቤ በማስገባት ቀናና እውነተኛ መልስ በመስጠት እድትተባበሩን እንጠይቃለን::

ማሳሰቢያ:-

- የሚሰጡን መልስ በሚስጥር የተጠበቀ ነው::
- ስም መጻፍ አስፈላጊ አይደለም::
- መልስዎን በጥያቄው ፊት ለፊት ባለው ባዶ ቦታ የ "✓" ምልክት በማድረግ ያስቀምጡ::
- ለትብብሮ በቅድሚያ እናመሰግናለን::

<u>ትዕዛዝ 1</u> :- **ከዚህ በታች ያሉት ጥያቄዎች ስለግል መረጃ የሚጠይቁ ሲሆን ከጥያቄዎቹ ፊት ለፊት ባለው ባዶ ቦታ ትክክለኛዉን መልስ በመሙላት ይመልሱ::**

1. **<u>የግል መረጃ (PERSONAL INFORMATION)</u>**
   - 1.1. ዕድሜ _____ ፆታ _____
   - 1.2. ተማሪ/ሰራተኛ_____
   - 1.3. የተመረቁበት የትምህርት አይነት_____
   - 1.4. የሚማሩት የትምህርት አይነት_____
   - 1.5. የስንተኛ ዓመት ተማሪ ነህ/ነሽ(ለተማሪ ብቻ)_____
   - 1.6. የትምህርት ደረጃ (ለሰራተኞች ብቻ) _____
   - 1.7. የስራ ልምድ(ለሰራተኞች ብቻ)_____

ትዕዛዝ 2፡-ከዚህ በታች ላሉት ጥያቄዎች በጥያቄው ፊት ለፊት ባለው ባዶ ቦታ የ "✓" ምልክት በማድረግ መልሶትን ይስጡ::

	ጥያቄዎች	አዎን	አይደለም::
1	የመረጃ ደህንነት ማለት ምን ማለት እንደሆነ አውቃለሁ::		
2	ከምሰራበት ስራ ጋር ስላለው የመረጃ ደህንነት ግንዛቤ አለኝ::		
3	የምሰራበት የጤና ተቋም ስለመረጃ ደህንነት ግንዛቤ ያለው ሰው ወይም ቡድን ወይም አሠራር አለው ::		
4	የምሠራበት የጤና ተቋም ስለመረጃ ደህንነት አጠባበቅ የወደፊት እቅድ አለው::		
5	የምሠራበት የጤና ተቋም በፅሑፍ የተዘጋጀ የመረጃ ደህንነት አጠባበቅ ፖሊሲ አለው::		

ትዕዛዝ 3፡-ከዚህ በታች ላሉት ጥያቄዎች በጥያቄው ፊት ለፊት ባለው ባዶ ቦታ የ "✓" ምልክት በማድረግ መልሶትን ይስጡ::

	ጥያቄዎች	በጥብቅ አልስማማም::	አልስማማም::	እርግጠኛ አይደለሁም::	እስማማለሁ::	በጥብቅ እስማማለሁ::
1	የአንድን መስሪያ ቤት የመረጃ ደህንነት ፍላጎቶች መደንገግ ተገቢ ነው::					
2	የመረጃ ደህንነት ምንነት እንደ ሙያዊ እውቀት መታየት አለበት ::					
3	የመረጃ ደህንነት እንደ ማንኛውም የሆስፒታሉ ስራ መታየት አለበት::					
4	የመረጃ ደህንነትን በጤና ተቋማት መተግበር ተገቢ ነው::					
5	በሆስፒታሉ መጠቀም ስላለብኝ የመረጃ ደህንነት ስልጠናዎችን ወስጃለሁ::					
6	በምሰራበት የጤና ተቋም ስላለው መረጃ አያያዝ ኃላፊነት አለብኝ::					
7	አመራሩ ለመረጃ ደህንነት አተገባበር እገዛ ያደርጋል::					
8	አመራሩ የመረጃ ደህንነት አስፈላጊ ነው ብሎ ያምናል::					
9	የምሰራበትን ሆስፒታል የመረጃ ደህንነት ፖሊሲና ህግጋት አከብራለሁ::					
10	የምሰራበትን ሆስፒታል የመረጃ ደህንነቶችን አያያዝ ማክበሬን ይከታተላል ወይም መከታተያ መንገድ አለው::					

11	ሆስፒታሱን የሚመለከት ማናኛውም መረጃ ከድርጅቱ ውጭ ላሉ ሠራተኞች ክፍት መሆን አለባቸው።					
12	ሆስፒታሱን የሚመለከት ማናኛውም መረጃ ለሠራተኞች ክፍት መሆን አለባቸው።					
13	የሆስፒታሱን የመረጃ ደህንነት ፖሊሲ ባላከብር ተጠያቂ መሆን አለብኝ።					
14	የመረጃ ደህንነት መረጃዎችን በቀላሉ ኮፒ ማድረግ እችላለሁ ።					
15	የመረጃ ደህንነት ፖሊሲን በተገቢው መንገድ ተግባራዊ ለማድረግ አሰራሮች ተዘርግተዋል።					
16	ለመረጃ ደህንነት ወጪዎች አመታዊ በጀት መመደብ ተገቢ ነው።					
17	የማከናውነው ሥራ የመረጃ ደህንነትን በሚያረጋግጥ መልኩ ለማስኬድ ዝግጅት አድርጋለሁ።					
18	የሆስፒታሱ አስተዳደር የመረጃ ደህንነትን ጠቀሜታ ይገነዘባል።					
19	የሥራ አመራሩ የመረጃ ደህንነት መረጃን በተዋረደ ለሁሉም የሥራ እርከን በአስፈላጊነት መንፈስ ያስተላልፋል።					

Annex 3. Guideline for in-depth interview.

For medical director

Main topics

1. Do you know what it means by information security?
2. Do you realize the importance of information security to your hospital?
3. What are the challenges for creating strong information security culture in your hospital?
4. What are the factors that contribute for the degradation of information security culture?
5. Do you have any mechanism that you implemented to secure information in your hospital?
6. Do you have information security policy developed and implemented at the hospital level?
7. What do you propose for betterment of the situation in the future?
8. What are your future plan regarding creating good information security culture in the hospital?

1. For medical record and human resource department heads

Main Topics

1. Do you know what it means by information security?
2. Do you realize the importance of information security to your hospital?
3. What are the factors that may possibly create loss or damage to information and information resources to your hospital?
4. Do you have any mechanism to protect information in your hospital?
5. What do you propose for betterment of the situation in the future?

Declaration

I, the undersigned, declare that this thesis is my original work in partial fulfillment of the requirement for the Degree of Masters of Science in health informatics and has not been presented for a degree in this or any other university. All resources of materials used for this thesis and all the people and institution who gave support for this work have been dully acknowledged.

Name: - Temesgen G.

Signature: - _____

Place: Health Informatics Program, Faculty of Informatics, Addis Ababa University.

Date of submission:- 13/07/2010

This thesis has been submitted for examination with our approval as the university advisor.

Name of the adviser:- Lemma Lessa

Signature:- _____ Lemma June 28/2010