International Journal of Trend in Scientific Research and Development (IJTSRD)

International Conference on Advanced Engineering and Information Technology (ICAEIT-2017)

ISSN No: 2456 - 6470 | www.ijtsrd.com | Special Issue Publication

Electronic Healthcare Record Security and Management in Healthcare Organizations

Attahiru Saminu, CLN
Department of Library and Information Science, College of Science and Technology
Hassan Usman Katsina Polytechnic Katsina State, Nigeria

ABSTRACT

This study aim sat identifying the current countermeasures used in protecting the Electronic Healthcare Record and how employees share their knowledge about the existence Electronic Healthcare Record security as well as countermeasures used in mitigating the threats and data breaches in healthcare organizations. A case study of Aminu Kano Teaching Hospital, Nigeria was used and qualitative research method was adopted where purposive and stratified random sampling was used. This led to construction of eleven relevant questions to four categories of staff. A conceptual frame work was proposed to quid the study and the findings we reevaluated using the proposed frame work. There sults revealed that there is lack of knowledge sharing among employees and some factors were found to be the resistance factors, this include educational background, behavior, low security awareness, personality differences and lack of management commitment. On the other hand, deterrent, preventive and organizational actions were partially practiced as countermeasures used to mitigate the threats and vulnerability of data breaches of Electronic Healthcare Records in Aminu Kano Teaching Hospital in Nigeria.

Keywords: *Electronic Healthcare Records, Security and Management, Countermeasures, Knowledge Sharing*

1. INTRODUCTION

Nowadays, using information systems in the healthcare environment provides many potential benefits such as improving the quality of care, reducing medical errors, enhancing the readability, availability and accessibility of information (1). However, Healthcare Information Systems (HIS) security threats have increased significantly in recent years. For instance, during the period from 2006 to 2007, over1, 5millionnames were exposed during data breaches that occurred in hospitals alone. The security challenges differ from one country to another country which includes lack of patient unique identifier, inadequate healthcare policies, lack of full acceptable global standards and privacy,

The common threats are computer crimes, hackers, computer viruses, Therefore, enforcement required for other countermeasures and other security and privacy regulations include firewalls, anti-virus, and intrusion, detection, and control systems are no longer given the required levels of detail protection. For this, (5) noted that the level of information security threats might increase due to the present Trans formation. Threats to Electronic

The best solution for this is by creating awareness to healthcare employees with knowledge of information security. Inanition, knowledge sharing among employees in healthcare organization could be challenging as their background and domains may differ. Moreover, organizations with low level so fIS security will face numerous of computer abuse and other confidentiality and security threats, According to (2) organizations spend a lot of money in order to ensure that their information systems are both protected from various types of attacks and incompliance with applicable laws. Despite all of these efforts, security breaches are still on the rise.

For example, (3) the study quoted a CERT (Coordination Center Survey Report) which showed that the number of reported security breaches by various organizations in the United States of America (USA) roseto137,529 in 2003 from 2,573 breaches reported in 1996. The challenge grows due to the fact that the types of threats change at the same pace with which the technology advances (4).

Medical Records (EMR) could be classified into two broad areas: (1) Organizational threats that started from the improper access of patient records by either internal agents misused their privileges or external agents abuse their vulnerability of information security systems, and (2) Systemic threats that occur from an agent in the information flow stages exploiting the disclosed data beyond its wanted use (6).

Security incidents, so it is very important for the IT organizations concerned to know what kinds of security measures that are effective in protecting information systems and data in their respective organizations. This paper focuses on the countermeasures that are used to help in mitigating security challenges in Healthcare organizations.

1.1 Research Objectives

The main objective of this research his to propose a frame work that can be used to improve Information System Security in Healthcare organizations.

OTHER OBJECTIVES INCLUDE:

1.2 Research Questions

a. What are the problems of information management in the investigated are a regarding Information security?
b. How these problems can be solved to improve information security?

THIS LED TO INVESTIGATE THE FOLLOWING:

1. To identify the Information Security countermeasures that healthcare organization use to mitigate security threats.
2. To identify the ways employees share knowledge about information security issues and countermeasures.
3. To evaluate the effectiveness of information Security countermeasures based on the proposed frame work from AKTH perspective.

1. How information security countermeasures mitigate the security threats of Electronic Medical Records?
2. How employees do share knowledge about information security countermeasures?
3. How information security countermeasures can be improved to solve the problems?

1.3 Related work

(3) Defines security as the state of being secure or free from danger and recognizes information security as just one of the multiple layers of security required among others like physical security, personnel security, operations security, communications security, and network security. (4) Describes information security as protecting information and information systems from unauthorized access, use, disclosure, disruption, alteration, and destructions,. All the above authors enumerate import ant characteristics of information albeit With variations.(5) List Confidentiality, Integrity, Utility and Possession as the critical characteristics of information while (4)recognizes what he calls Parker Ian Hexed, which takes Confidentiality, Integrity, and Availability, called CIA triangle (6)add Possession, Authenticity, and Utility. Confidentiality is concerned with the responsibilities of the custodian of other people's personal data as opposed to privacy which is associated with a person's control over his or her personal data (7).

Information systems security can be categorized into physical and technical securities. Information Technology (IT) security can be computer and communication system security. It is positioned towards what the overall security requirements should be. This part of the overall security is thus at an organizational level and concerns the business sasa whole (8).Computer Security concerns with the protection of hard ware and its contents while Communication Security includes the Protection of networks and other information media that communicate information among computers, In order to provide a more understand able view of how these characteristics and security measures relate to one another, an information security model has been created. The aim of the model is to describe what information security represents. The model combines the definitions and descriptions mentioned above.

Information Systems effectiveness has been extensively studied over the past years because of its importance in the field of Information Technology (9). However, there is a lack of understanding and knowledge on how security measures and organizational factors can influence the level of security effectiveness in Information Technology (IT) organizations in the current literature (8)and(10) suggested that information system security administrators consider the following to improve the Information System security level in their organizations.

1. Information Technology (IT) organizations should monitor and enforce policy and distribute information about organizational guidelines for acceptable system usage.
2. Environmental factors such as the tightness of the security environment and visibility of the Security administrators should be taken in to consideration to reduce the number of computer abuse incidents
3. Information Technology (IT) organizations should put it more effort in security issues by expanding the staff hours on IS, security.

They further proposed a conceptual frame work for effective information system security in Information Technology (IT) organizations that includes: Disincentives Certainty, Systems Environment Security Control, Codes of Ethics, Software Security Controls, Top Management Support and Organizational Maturity were considered as independent variables that have an impact on a security effectiveness.

Many researchers agreed with the idea that the human mind is composed of rational and emotional components. A few authors state that security behavior depends on a person's attitude and beliefs. Believe is cognitive information without an emotional component, but the attitude is an evaluation or emotional response (11). Some other author's (12) proposed the ABC Model where employee attitude to information security issues is based on rational component (cognition) emotional component (affect) and behavior.

A. Emotional aspect of attitude for example, for Example, feeling like grief, pain, fear, guilt,
B. Behavior component is derived from fact that our behaviour also gives feedback to attitude
C. Cognitive or thoughtful aspect of attitude.

The implementation of health information technology and electronic exchange of patients' information will result in privacy violations and security breaches. For information security, knowledge sharing is Significant to make sure that the knowledge can be transfer among employees, disseminate and distribute to make it available to those who require it (13). Mean while in (14), they have identified that knowledge gap and flow as part of knowledge sharing among healthcare providers analysis. (15) Adopted Nonaka's modes of knowledge creation between tacit and explicit knowledge to ensure that knowledge can be created and disseminated. (13) Identified the key resistance factors in knowledge sharing towards information security culture in the healthcare organization. Some key resistance factors highlighted are the lack of top management commitment, behavior, lack of trust, personality differences, and lack of communication, low-security awareness, cultural differences, and openness to experience.

There view of the literature has explored four (4) main areas of information system security in healthcare organization. This includes Information Security System Model that work on two different levels: system level and process level; the system level contains the process of level tasks and it has been included organizational Structure, process and resources, This is designed to establish, monitor, implement, operate, maintain and improve the characteristic of information security by the collaboration of different activities while the process level concerned with the development, implementation, planning, maintenance and evaluation of the IT security.

The End User Security Behavior that composed of rational and emotional components of human mine where it employs attitude to information security issues based on the emotional spect of attitude, for example, Feeling like grief, pain, fear, guilt, the behavior component that derived from the facto four behavior also gives feed back to attitude and the cognitive or thoughtful aspect of attitude.

The Knowledge Sharing in Information Security Systems tries to ensure that the knowledge can be transfer among employees, disseminate and distribute to make it available to those whore quire it. This identified the key resistance factors in knowledge sharing towards information security culture in a healthcare organization. Some key resistance factors highlighted are the lack of top management commitment, behavior, lack of trust, personality differences, and lack of communication, low- security awareness, cultural differences, and openness to experience.

Finally, is the Information System Security in IT Organization suggested that Information System security administrators should consider the Disincentives Certainty, Systems Environment Security Control, Codes of Ethics, Software Security Controls, Top Management Support and Organizational Maturity to improve the Information System security level in their organizations. In recognition of that, healthcare organizations heavily rely on generating patients' data, therefore, these will. Play a significant role to protect the information generated and understand the effective information security management in healthcare organizations. The literature studied offers in sight in to those challenges of information security and offers recommendations that have the potential to be further articulated and expanded to improve the security management in a health care organization.

Base on the literature reviewed, a conceptual frame work Information Systems Security (ICT-ISS Model) is developed that mapped Disincentives Certainty, Systems Environment Security Control, Codes of Ethics, Software Security Controls, Top Management Support, Organizational Maturity and Conceptual Model of Knowledge Sharing in to a single conceptual frame work for information security.

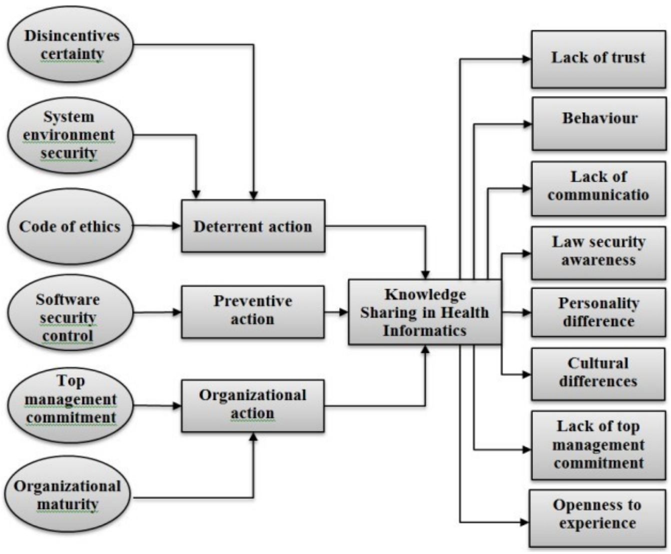

Figure 1 Information and Communication Technology Information Security System Model (ICT-ISS Model

2. Research Method

A qualitative study was conducted. "It seems Too obvious that, the choice of the research method ought to be determined by the nature of the research problem". (18), this is through an in-depth face-to-face interview with a total of 10samples,ascomprising of 2hospital personals representing both the system providers (Information Technology Manager) and the end-users (doctors, nurses, allied health personnel) in the. Oto rhino laryn go logy (ENT) department of AKTH .In addition, Information Technology Systems applied in above named hospital is at different stages of development and defers from one department to another. Therefore, the description on their departmental information system is based on the stage of implementation and its functionalities

The interviews were conducted in February, 2016. Purposive and stratified random sampling was used to select the samples among the hospital staff that are directly involving with the information system in the hospital. Once the identified sample verbally consented for the interview, an in-depth face-to face interview was

The data obtained was sorted according to various categories based on content analysis. Data

3. RESULTSAND DISCUSSION

Research question 1; how information security counter measures mitigate the security threats of Electronic Medical Records?

3.1 Deterrents actions

The literature suggested that deterrent action is necessary in order to discourage an individual from intentionally violating information security policies or procedures (13). Deterrent action is all about discouraging users from intentionally violating information security procedures or policies like computer security awareness, policy statements, guidelines, minimum standards for personnel behavior and organization personnel rules that may include some conditions for the appropriate way of system use, the main aspects of deterrent actions are:

There is a report that indicates that the employees of Aminu Kano Teaching Hospital (AKTH) are misusing EHR soft ware and at times in stalled illegal soft ware for their personal used. However, no any punishment or penalty attached to that misconduct. Furthermore, there is no available IT staff to monitor and ensure the server rooms are saved and secured every time and to make sure that.

The current study, further, suggests that immediate adoption of deterrent actions may have direct significance to reduce the level of security threats. This is by applying the key content so fit, by both the IT engineers, medical staff and the top management intern of providing computer security awareness training, guidelines, policy statements and a minimum setoff standards for personnel behavior and Performed in their respective units, The samples were introduced to the interviewer and were briefed about the study purpose. The interview was conducted using an identical guide questions to ensure similarity of interviewing method and flow of discussion Analysis was carried out by using N vivo soft ware and mapping according to emerging themes.

1. Disincentives certainty that takes care of punishment and penalties up on violating any rule and this will discourage individuals from violation of such laws
2. System environmental security refers to the tightness on the visibility of the security managers and security environment that may reduce computer abuse
3. Codes of ethics are the rules and standards governing the conduct of an employer with others

only authorized users are allowed to those server rooms but unfortunately, everyone has access to those server rooms.

By observations, AKTH has no any program at hand that incorporated the IT employees with other healthcare stakeholders. So actually, there is a gap between IT staff and other employees with regards to the security of EMR
Security in AKTH

Company personnel rules that contain specific conditions for the accept able use of the system. The findings are also consistent with the findings from Information System Security Countermeasures literature (18; 17) pointed the impact of deterrent actions to healthcare organization throughout the medical processes.

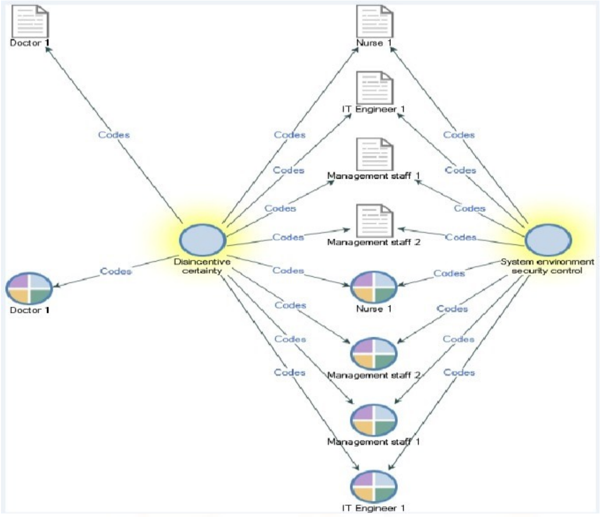

Figure 2 Shows response on Disincentive certainty and system environment control

3.2 Prevention actions

Preventive Actions Currently IT security measures are provided by both operating system and data base management systems security software access control Password control is used to prevent unauthorized access and misuse of computers. For website security purposes, the MIS unit has compiled a script in UNIX.

Information System Security Counter measures are necessary with the prevailing of Electronic Medical Records threats. Preventive actions enable only authorized users to access a computerized system (8). Preventive coition allows access to a computerized system by only authorized users. The main concerned is on the software security controls that comprise operating system security Software control, fourth generation security software control, DBMS security software control and specialized security software control. Preventive action increases the level of security effectiveness's through the use of software controls intended to inhibit free use of computing resources

The study investigated four types of preventive actions: the DBMS security software, fourth generation security software, specialized security software and operation system security software. Where found the partial application of DBMS security software and specialized security software by IT staff, Doctors, and Management Staff, preventive actions is a very important full application of it will provide security to entire systems. The use of password will enable only authorized users to have access to their system but in AKTH employees have access to their each other systems without out the use of any personal password.

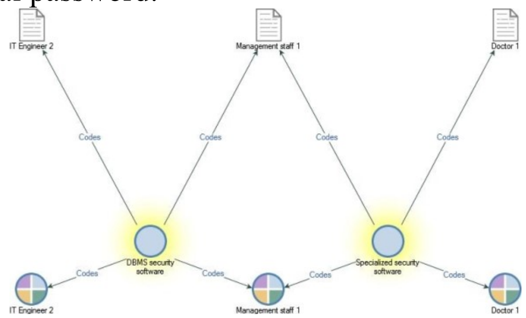

Figure 3 shows the rate of Prevention actions

3.3 Organizational actions

The organizational objectives are to maintained and develop legal and high-quality services. The findings of this case study revealed that when proper an a gement activities are implemented they lead to the intended objective of EMR security. Such activities include top management support and organizational maturity. Top management support indecision making, monitoring security measures, encourages employees to comply with security rules and procedures. The mature organization is the one with formalized business's procedures and guidelines, high use of performance measurements and availability of decision-

This study suggests that top management commitment may have the direct impact on the level of information security measure. This can be achieved through top management's willingness to exert the required effort, in terms of allocating the righter sources and making decisions insecurity related issues. Furthermore, it is also suggested that immediate manager's commitment to mature organization's information security program .In terms of consistency and enforcement of the rules implemented, appeared to have a direct impact on the top management's commitment to the development and deployment of the related data. The findings related to the suggestion made in the literature as "it is quite that mature organizations have proper guidelines and code of ethics that will stress on the proper and improper usage of information systems thus increase the level of security effectiveness."(13). It was observed that AKTH management staff has neglected the issue of EMR security control. However, there are many incidences of security violations like free access to computerized systems and many other offenses committed by the employees but no any actions were taken to ensure the security of such system. Even though, some rules and procedures a rewritten but no implementations and enforcement to the employees. Organization's Electronic Medical Record Security. This is because of a good relationship between managers and employees. These findings also are in line with "Healthcare organization that aimed to apply KM strategy and integrated with knowledge sharing needs to focus more relationship between managers and employee. These may help to improve the organization's current security knowledge and requirements among healthcare practitioners in cultivating information security culture." (19)

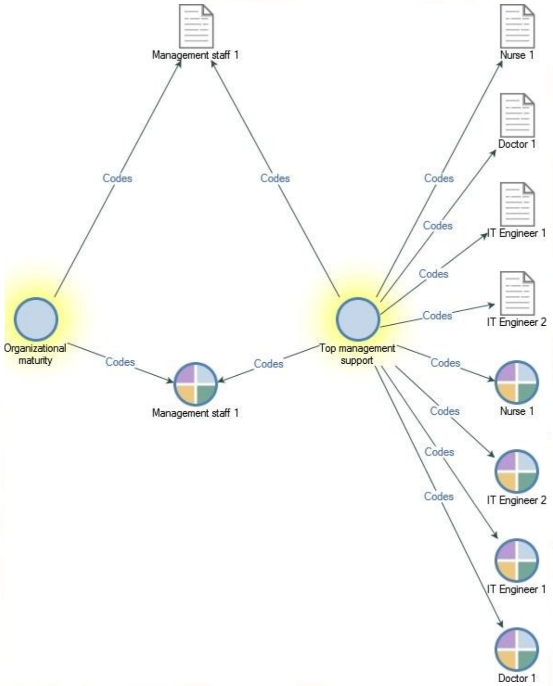

Figure 4 shows the Organizational actions

3.4 Knowledge Sharing Towards Information Security Culture in Aminu Kano Teaching Hospital

The study suggests that there should be a proper knowledge sharing of information security measures and knowledge in terms of formal and informal that is individual's willingness to share. Moreover, there were neither formal no informal mechanisms for sharing information and knowledge with regards to EMR security countermeasures and other related issues between the IT staff and other AKTH employees. Impact; there were no organizational strategies in place to establish priorities for

Research question 1: How employees do shared knowledge about Information Security countermeasures?

Information and knowledge sharing issues or for how it should be utilized. It was also observed that while a little Informal sharing existed between management and IT staff, the same time limited to medical staff.

The observation from this study also pointed some factors that affect tproper Knowledge sharing with regards to EMR security counter measures. For Example, the study revealed that some members are willing to share but due to some key resisting factors they couldn't do so among which are behavior, educational background, personality differences and lack of top management commitment. These findings are also in line with (5) "The key resistance factors identified are; Behavior, Lack of top management commitment, lack of communication, low-security awareness, personality differences, cultural differences and lack of trust, openness to experience

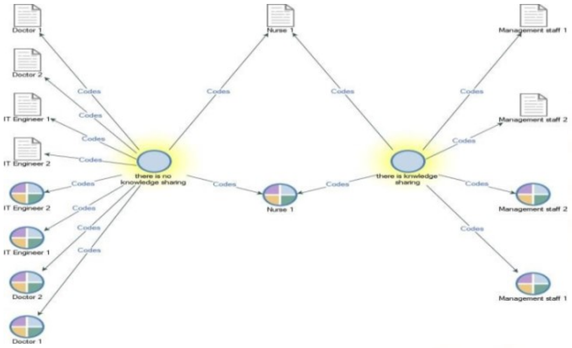

Figure 5 Shows the comparison between there is and there is no knowledge sharing

In general, the findings obtained revealed that the respondents are on the same view of Disincentive certainty, System environment security control, DBMS security software, Specialized security software, Top management support, and Organizational maturity are the countermeasures widely used in Aminu Kano Teaching Hospital (AKTH) as summarizedinTable1 below, similarly, other countermeasures like code of ethics, Fourth generation security software and Operation system security software were neglected in Aminu Kano Teaching Hospital (AKTH). The following matrix table shows the key findings for each concept are succinctly summarized. The summary indicated in the below matrix table was compiled base on participant's data found that described the response rate of each interviewe

VARIABLES			RESPONDENTSRATE						
Deterrents actions		IT1	IT2	Doc1	Doc2	Nur1	Nur2	MGT1	MGT2
1	Disincentive certainty		×		×				
2	System environment security control		×	×	×				
3	Code of ethics.	×	×	×	×	×	×	×	×
Preventive actions									
1	DBMS security software	×		×	×	×	×		×
2	Fourth generation security software	×	×	×	×		×	×	×
3	Specialized security software	×	×		×	×	×		×
4	Operation security system software	×	×	×	×	×	×	×	×
Organizational actions									
1	Top management support				×				×
2	Organizational maturity	×	×	×	×	×	×		×

Source: concept matrix table. Colin's, (2013)

Base on the above evaluation and comparison of the proposed frame work and the result found, a new framework was analyzed (see Figure 6). The countermeasures found were a link to the knowledge sharing that will lead to effective security of Electronic Medical Records in AKTH.

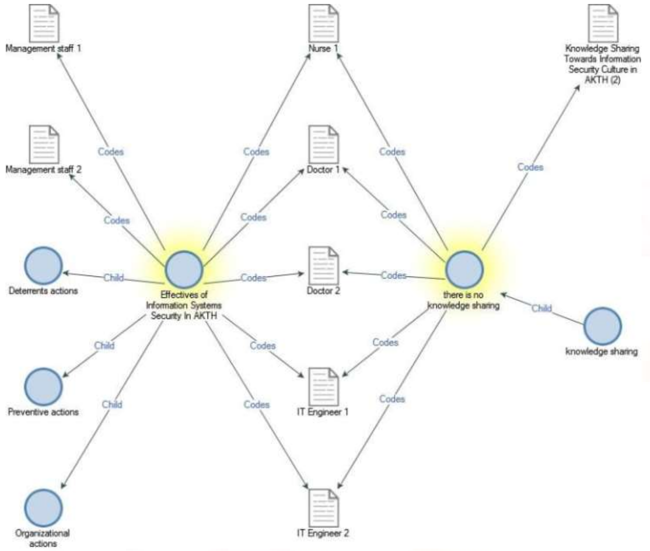

Figure 6 effective information securities through knowledge sharing

The findings of the fund a mental research as well as the empirical study provided an undisputed agreement for supporting the information Systems Security model introduced by this research. Both frame works, the Effectiveness of Information Systems Security mode land knowledge sharing model mapped in one mainframe work were consolidated in one main frame work that could be Used to deploy an effective information security countermeasure, Moreover, the introduced frame work is a step towards a theory of Effectiveness of Information Systems Security countermeasures; As such the study has drawn a variety of theories from many aspects of information system security.

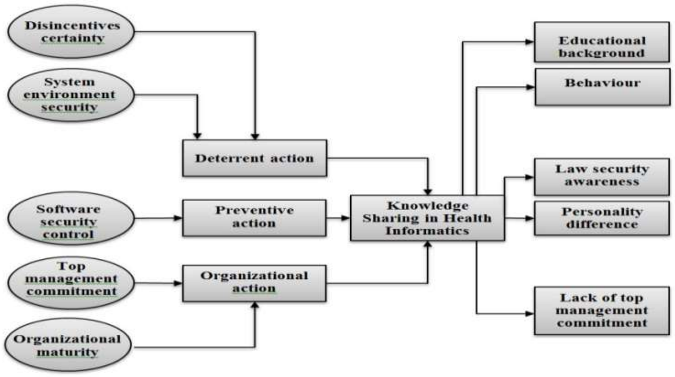

Figure 7 Evaluated ISS (ICT-ISS Model)

4. Conclusions

The state of information security at Aminu Kano Teaching Hospital is beneath minimum standard required by international information security standards and other dependable information security organizations and authors. In effect, information resource sat Aminu Kano Teaching Hospital are somewhat vulnerable. The healthcare environment play san import ant role due to its need for openness, and diversity of users and their needs

The main challenges to information security have been identified as follows.

1. Lack of strong policies/strategies/framework/standards Law top management commitment towards effective information security measures
2. Law security awareness/knowledge sharing on the existence of information security countermeasures among employees
3. Inadequate qualified and IT skilled staff Ineffective information security countermeasures to tackle security threats to Electronic Medical Records.

5. Recommendations

a. Provision of effective countermeasures, committed leadership, full awareness, standard, policies, laws and guidelines
b. Immediate adoption of deterrent actions may reduce the level of security threats. In term of providing computer security awareness training In term of providing computer security awareness training for personnel and company personnel rules for the use of the systems.
c. Except these issues are immediately consignor mitigated, the security of information assets at Aminu Kano Teaching Hospital can never be assured
d. Preventive actions is very important full application of it will provide security to entire systems
e. Immediate manager's commitment to mature organization's information security program. Like consistency and enforcement of the rules Implemented,

REFERENCES

1. HIT&MIS: A statistical Analysis of Disclosed Storage Security Breaches. **G, Goldschmidt P.** s. l.: ACM, 2006.
2. Health Information Engineering and Systems (FHIES), Computer Science, 2012, 7151, p195-206.**DongN, Jonker H, Pang J.** s. l.: USENIX, 2012, Vols.7151, 195-206.
3. **Kok OM, BasogluN, Daim, T.** Exploring the Success Factors of Electronic Health Record System Adoption, ProceedingsofPICMET'12:

Technology Management For Emerging Technologies, Turkey: Bogazici University, 2012.

4. **Kruger H&KearneyW.** A prototype for assessing information security, Computers andSecurity,.2006.
5. A Conceptual Model for Knowledge Sharing To wads Information Security Culture in Healthcare Organization, Hassan, etal**, (2013),** 2013, IEEE 3rd International conference on research and innovation systems (ICRIIS'13), 5,
6. Investigating Barriers to Electronic Medical Record Use during Collaborative Information Seeking Activities. **KarunakaranA, YoungHN, MadhuR.** s. l.: The 2nd ACM SIGHIT International Health Informatics Symposium, 2012, Vols.p.743-748.
7. A prototype for assessing information security. **Martin &Kruger H&KearneyW.**2006, Computers and Security,, Vol.25($),pp.289-296.
8. The Basics of Information Security: Understanding the Fundamentals of Information Security in Theory and Practice. **Andress.**2011, us a. eLSEVIER.
9. Principles of Information Security:. **Wihitman& Mattord.** 2005, Course Technology. Boston.
10. ‘Privacy: Aspects, definitions and a multi-faceted privacy. **Renaud& Galvez-Cruz.**2010, Information Security for Sourth Africa,, pp.1-8.
11. **Wallin.** Managing Information Security in Healthcare: A Case Study in Region, Skåne, Master Thesis,. 2008, pp.11-12.
12. "Introduction to computers and information" .**Wise & Athey.**2003, IEEE Journal, 309-315.,pp. 309-315.
13. Effective of Information Systems Security in IT Organizations in Malaysia. **Al-Salihy.** Malaysia: s. n., 2003.9thAsia Pasific Conference on Communications APCC, 5.
14. **Kabay, M.E.** Using social psychology to implement security policies, Computer Security. s. l.: Handbook. www.mekabay.com/infosecmgmt/SocPsychINFOSEC pdf, 2002.
15. Cultivating an organizational information security culture. **Tipton, H. F. & Krause M.** s.l.: Computer Fraud &Securiyty,7-11.,2006,Computer Fraud& Security,, Pp.7-11.
16. “Knowledge Management Barriers: An Interpretive Structural Modeling Approach”. **M. D. Singh and R. Kant.** 2007. IEEEInt. Conference in Industrial Engineering and Engineering.
17. **Lupiana.**“Development of A Frame work To Leverage Knowledge Management Systems to Improve Security Awareness”. s. l.: Dublin: Dublin Institute of Technology. 2008.
18. Librarians, Professionalism and Image: Stereotype and Reality, Library. **Luthmann, Abigail.**9, 2007, Review, Vol.56, p.775.