INFORMATION SECURITY RISKS INVOLVING FUNSOFT AS A HEALTH MANAGEMENT INFORMATION SYSTEM

Peter Migoya Halwenge, S. O. Liyala and George Raburu

School of Informatics and Innovative Systems

Jaramogi Oginga Odinga University of Science and Technology

P.O. Box 210-40601, BONDO-Kenya

ABSTRACT

This study looked at the various information security risks brought about by the implementation of funsoft which is a health management information system with a view of managing and mitigating the risks in a coherent and systematic manner. The study has used a positivist approach with a research design that employed quantitative descriptive study of funsoft users and focus group discussions with system administrators and records officers. The study population was eighty five with a sample size of forty six calculated using Yamane's formula with a precision of ten percent. The study reviewed current risk management practices used within the HMIS and IT in general and using a case study of three public hospitals in Kisumu county that are at different implementation levels of funsoft, it further explored current potential obstacles encountered in the implementation of systemic risk management strategy. This study finally implemented a strategy for managing risk within funsoft in a systematic and continuous manner which was enriched by material documented in the literature. It was unearthed in the study that all the three health facilities have no focal person to coordinate information security, lack policies and procedures on computer and information security and had never undertaken a risk assessment of the funsoft HMIS platform since its deployment.

INTRODUCTION

The need to secure information systems in any business setup cannot be undervalued anymore in today's information age. Scarfan and Hoffman (2009) reported that this was largely so because organizations are vulnerable to uncertainties whose impact may negatively or positively impact them in many ways. Mattrod (2009) further elaborated that the effects could be operational or financial and it was upon the IT security professional to help and support her organizations' management in the understanding and management of the uncertainties. This study therefore confirms that the proper acceptance of the impacts of information security would ultimately attain the critical dictum of information security that is to act as a critical piece for an institution attaining its business objective or in fact information security should be included as one of the managements long-term business objectives that is extremely dynamic in its form and nature. Alshaikh and Chang (2014) confirms the dynamicity of information risk and asserts that the management and mitigation of all risks an organization faces could be almost impossible as a result of the metamorphic nature of threats and vulnerabilities. Alshaikh and Chang (2014) points out that most organizations are incapacitated with limited resources making the management of risks a difficult task to accomplish largely due to the delicate tradeoff between the probable impacts against the cost of investment to cushion the impact. To this effect, Elky (2006), recommended that IT security professionals must have a toolset that is consistent, repeatable, and cost-effective that would reduce risks to a reasonable level to assist them on sharing commonly understood view with IT and Business managers in regards to the impact of various IT security threats to the organization's mission. To adequately develop an understanding of the risk management process, the study defined terms associated with risk management such as risk, vulnerability, threat, threat agent and risk management.

RESULTS AND DISCUSSIONS

4.2.2 Security Policy and Procedures as a source of risk

The bar graph below presents the various aspects regarding information security policies and procedures.

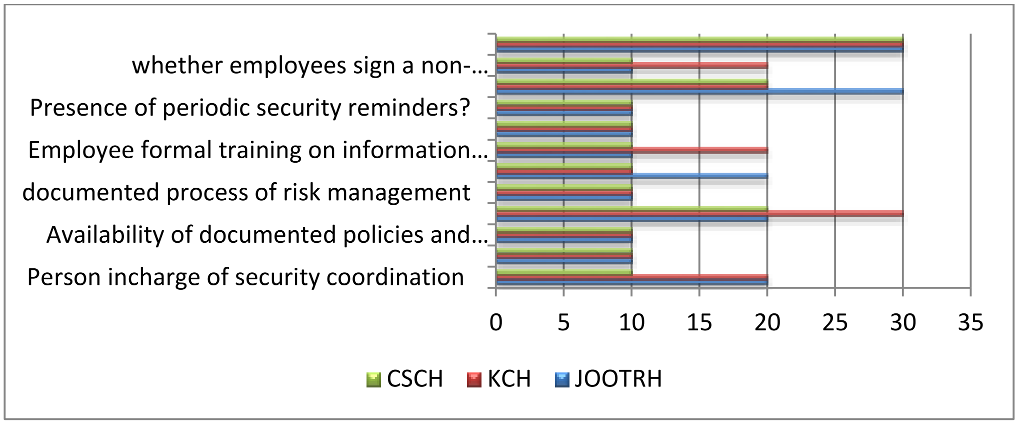


Figure 1 Information security policies and procedures Source: Author's Data (2014)

The graph clearly shows that CSCH has no person in charge of security coordination while at KCH and JOOTRH this duty is bestowed on the system administrators of the two facilities (partially addressed). A worrying scenario is found to cut across the three health facilities as they do not have any formal agreements with third party IT service providers who unfortunately are the suppliers of FUNSOFT and maintain the system periodically. This exposes the facilities to access of ePHI by the service providers. Other issues on security policies and procedures not addressed in the three health facilities are non-availability of documented policies and procedures, non-availability of documented process of risk management, non-communication of policies to employees and absence of periodic security reminders. The only concern that seems to be fully addressed is the presence of a formal physical security plan of the facilities.

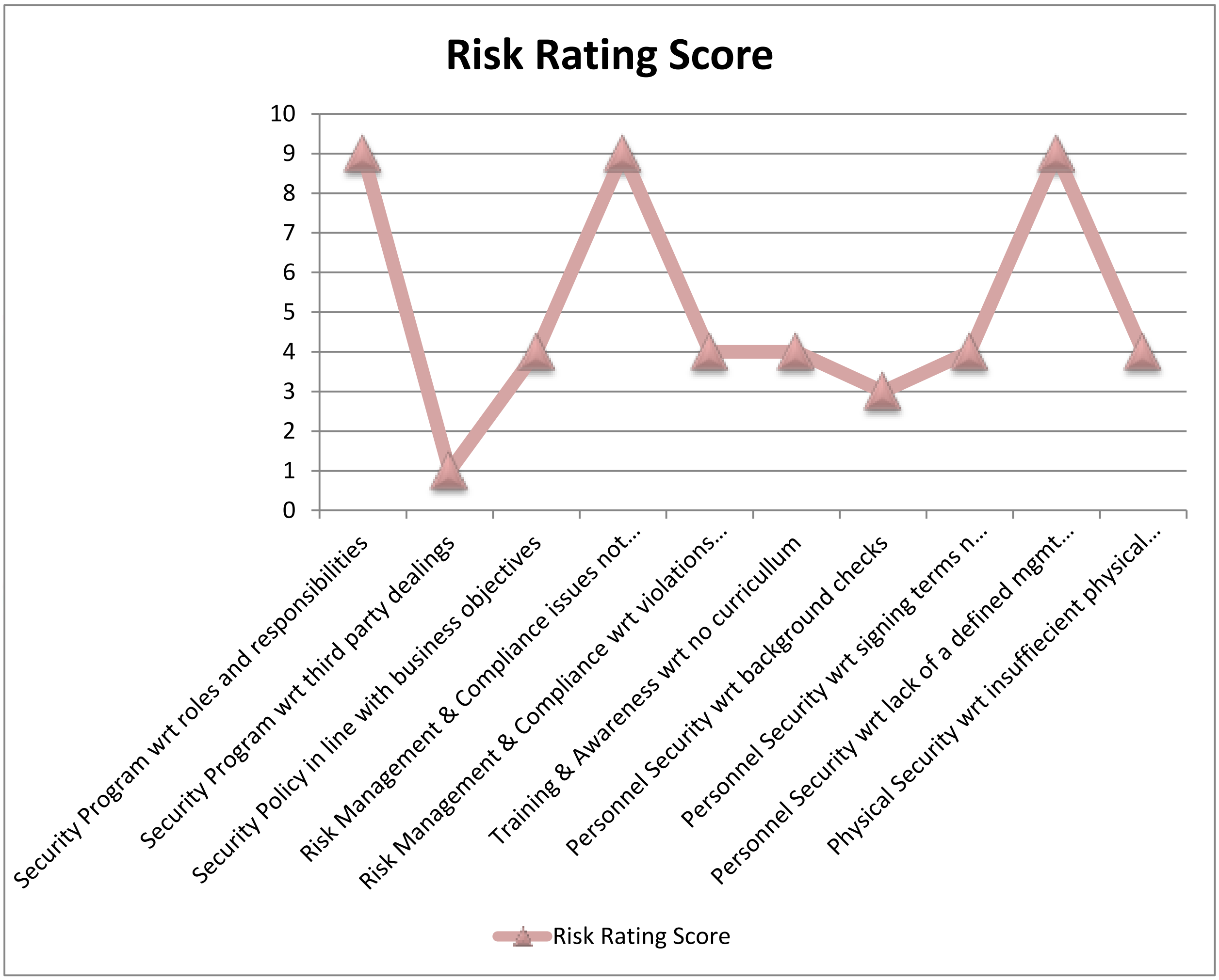


Figure 2 Risk rating score assignment Source: Author's Data (2014)

The above line graph shows that aspects security policies and procedures that are not addressed contribute to the highest risk ratings while those fully addressed minimally contribute to risk rating. The following can be summarized as overal findings around this category:

a. Security breaches are prevalent while dealing with IT service providers as third parties as a result of inadequate security measures in the associated third party agreements

b. Management is not briefed on information with regards to risks and related control measures prior to making management decisions.

c. Regulatory, legislative, contractual or statutory undertakings that relates to security are violated as a result of poor or inadequate controls.

d. Applications and technological solutions to harness risk are not properly used since there exists no formal training or curriculum on the same for employees

e. Terminations or change of responsibilities of employees or third party providers could result in a security violation due to lack of a predefined management procedure for terminations or changes in responsibilities.

4.2.3 Access Controls and Management as a source of risk

KCH has fully automated the process of identity and access management of its employees within the laboratory. This is a formal access authorization process based the principle of least privilege. JOOTRH and CSCH have partially addressed this concern. All the three facilities have partially addressed the issuance of uniquely identifiable user IDs to employees. The three health facilities have not also addressed the aspect of entitlement reviews which is a process of reviewing user accounts and corresponding access.

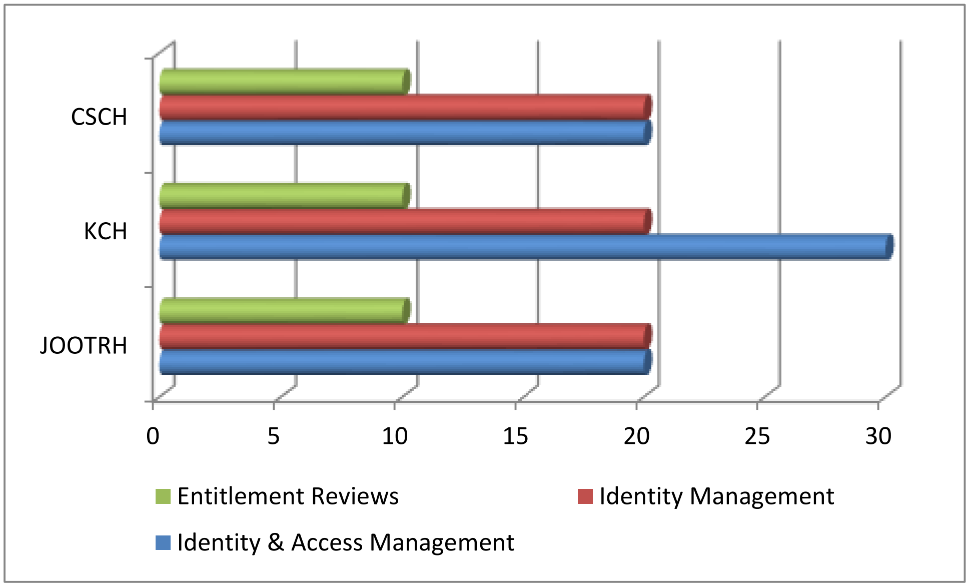


Figure 3 Access control and management Source: Author's Data (2014)

A further analysis based on the risk rating with logical access presents the scenario below where access by authorized user whose business use has expired as exposing the system most to unauthorized access (risk rating 9 high) while unauthorized users gaining access to the operating system with legitimate access is of low risk (3).

Table 1 Logical Access Risk rating Source: Author's Data (2014)

Logical Access Risk Rating	**Risk Rating**		
	JOOTRH	KCH	CSCH
unauthorized access to IS	Medium	Low	Medium
unauthorized users gaining access OS as authorized users	Low	Low	Low
access by an authorized user whose business use has expired	High	High	High

A very saddening situation was revealed by the Clinical officers who are interns on the use of passwords to the FUNSOFT platform. All the interns have been assigned one password that is pinned on the wall hence compromising the system immensely.

The following can be summarized as overal findings around this category:

a. Unauthorized access is gained to information systems.
b. Users whose responsibilities have change or no longer use the system still retain access to the information system.
c. Lack of consistent logging and monitoring mechanisms enables the continued unauthorized information processing activities to occur undetected.
d. Absence of clear segregation of duties compromises the integrity of the processes (for example. maker & checker).

4.2.4 Virus / Malware as a source of risk

When this issue was raised to the non ICT staff, almost half of them (43.5%) reported that it had been inadequately addressed. This opens a door of further possible attack to the FUNSOFT system as the malware protection has not been adequately taken into consideration.

Table 2 Virus / Malware protection Source: Author’s Data (2014)

reliable protection against malware and viruses

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	fully addressed	7	15.2	15.2	15.2
	Addressed	4	8.7	8.7	23.9
	partially addressed	12	26.1	26.1	50.0
	poorly addressed	20	43.5	43.5	93.5
	not addressed	3	6.5	6.5	100.0
	Total	46	100.0	100.0	

The same pattern of lack of protection against virus and malware attacks was evident from the system administrators response as JOORTH and CSCH rated the risk as high (9) while KCH rated the risk as medium (6).

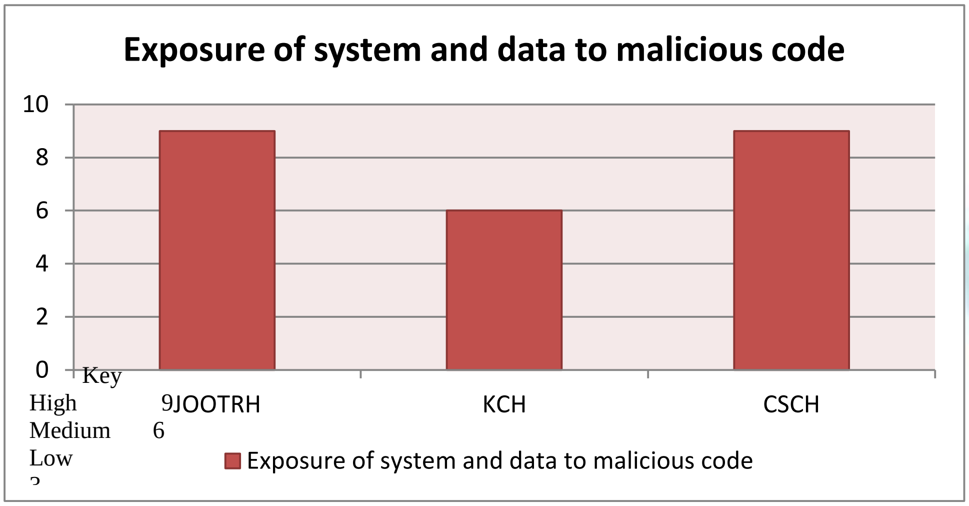


Figure 4 Exposure to malicious code Source: Author’s Data (2014)

4.2.5 Network Perimeter Security Control as a source of risk

A general observation from the respondents was that the network perimeter controls in place poorly address (45.7%) the security concerns. A sizeable portion of the same respondents were of the opinion that the network perimeter control addressed (28.3%) their security concerns.

Table 3 Network Perimeter controls Source: Author’s Data (2014)

reliable computer network perimeter controls

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Addressed	13	28.3	28.3	28.3
	partially addressed	9	19.6	19.6	47.8
	poorly addressed	21	45.7	45.7	93.5
	not addressed	3	6.5	6.5	100.0
	Total	46	100.0	100.0	

A critical analysis of this general opinion from the system administrators across the three health facilities revealed the key factors that enable or inhibit network perimeter controls. The figure below shows that the ability of intruders to exploit technical vulnerabilities to gain access to the system was most pronounced with a risk rating of 6 (medium) in all the three facilities under study. The location of sensitive systems vis a viz the less sensitive systems is an issue of concern at JOOTRH and CSCH (risk rating of 6 medium) as the facility reported incidences of locating sensitive systems in places respondents viewed to be less secure. KCH has tried to secure all its sensitive systems within the laboratory buildings that has both access control protection and 24 hour CCTV surveillance hence the low risk rating of 3.

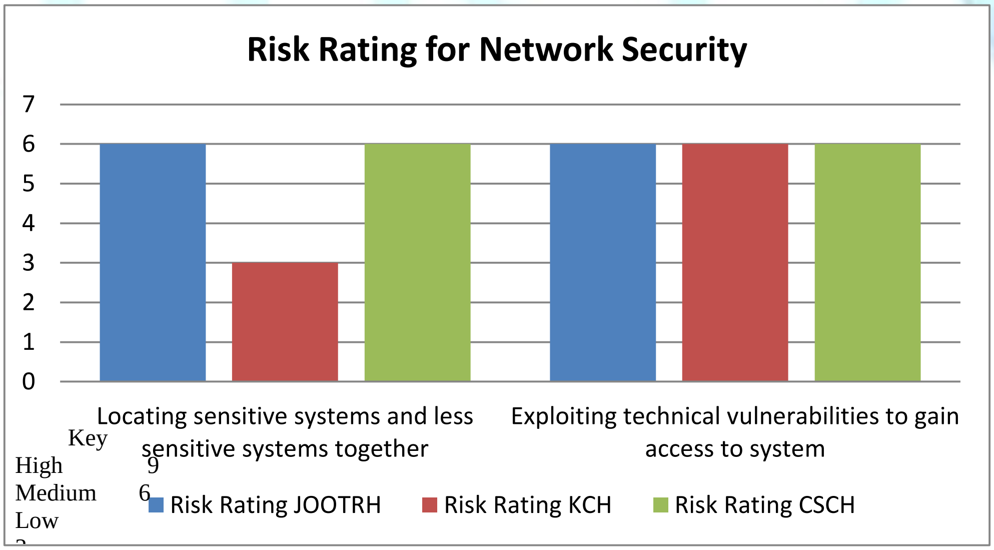


Figure 5 Risk rating for network security Source: Author’s Data (2014)

The following can be deduced as overal observations on this category:

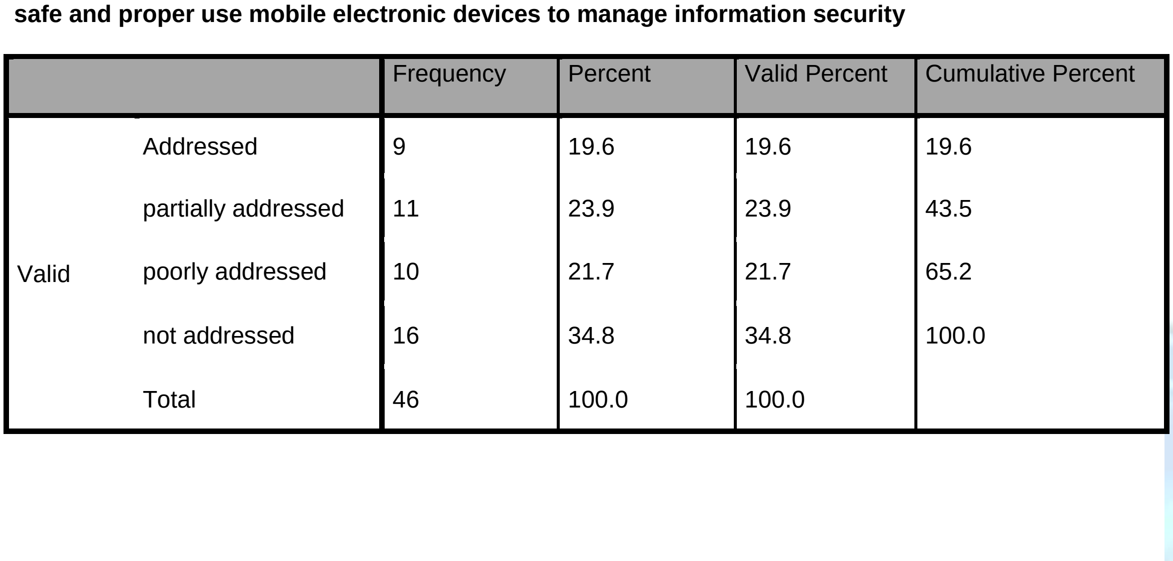
a. Unauthorized persons have access to sensitive systems which are located in the same place with less sensitive systems

b. lack of controls for technical vulnerabilities enables access to information by unauthorized persons

4.2.6 Portable Devices and Remote Access Security as a source of risk

The table below shows that the secure use of portable devices is not addressed (34.8%) while a good number report that it is partially addressed (23.9%) all the three health facilities under study.

Table 4 Use of portable devices to manage InfoSec Source: Author’s Data (2014)



safe and proper use mobile electronic devices to manage information security

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Addressed	9	19.6	19.6	19.6
	partially addressed	11	23.9	23.9	43.5
	poorly addressed	10	21.7	21.7	65.2
	not addressed	16	34.8	34.8	100.0
	Total	46	100.0	100.0	

A careful look of this general phenomenon from the system administrators across the three health facilities revealed the key factors that enable or inhibit remote access security are third party connections of IT service providers in all the facilities under study which compromises as it has a risk rating of 9 (high). Ineffective media handling procedures uniformly put the three facilities at risk (rating of 6 medium) while unauthorized access to data from discarded media minimally puts the systems at risk (rating of 3 low) most likely because HMIS is still a new concept under implementation.

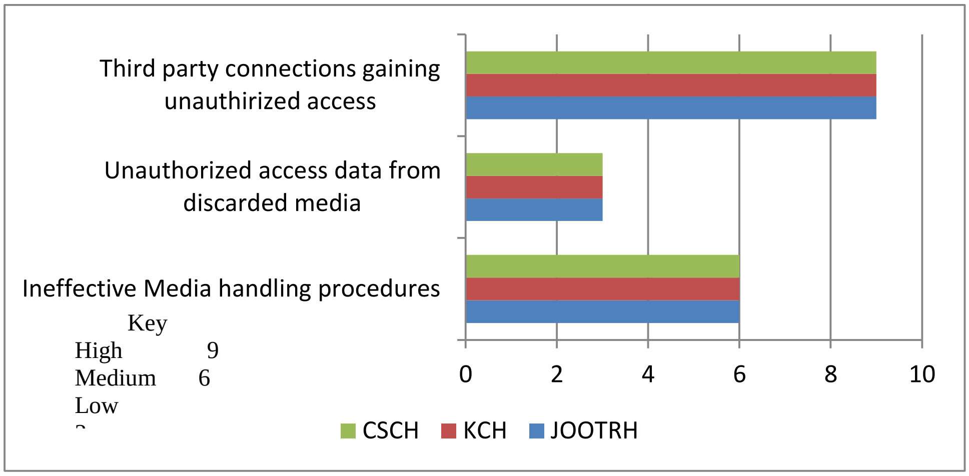


Figure 6 Media handling and remote access control Source: Author's Data (2014)

4.2.7 Secure Electronic Communication, Backups and Disaster Recovery Plans as a source of risk

When asked their perception on the safe and proper use of the email and internet, more than half (58.7%) of the non ICT staff reported that it was poorly addressed across the three health facilities. On further interrogation from them why this situation was at that state, it was discovered that use of the internet and email is only allowed administrative staff at the caliber of accountant, system administrator and hospital superintendent. This conforms to the small percentage of respondents who said it was addressed (8.7%) or partially addressed (10.9%). Limiting access to the internet and email would help the facilities void intrusion by external parties hence some semblance of information security assurance.

Table 5 Use of email and internet in conformity with hospital policies and procedures Source: Author's Data (2014)

processes for safe and proper use the internet and email in conformity with hospital policies and procedures for information security

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Addressed	4	8.7	8.7	8.7
	partially addressed	5	10.9	10.9	19.6
	poorly addressed	27	58.7	58.7	78.3
	not addressed	10	21.7	21.7	100.0
	Total	46	100.0	100.0	

On further prompting on whether the information flowing departmentally was secure, a good number of the respondents were of the opinion that was partially addressed or addressed totaling to 78.3% cumulatively.

Table 6 Reliable systems for secure sharing of confidential information Source: Author's Data (2014)

reliable system for secure sharing of confidential information

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Addressed	3	6.5	6.5	6.5
	partially addressed	33	71.7	71.7	78.3
	poorly addressed	1	2.2	2.2	80.4
	not addressed	9	19.6	19.6	100.0
	Total	46	100.0	100.0	

Questions were raised on whether the health facilities staff had knowledge of information backup. Almost half (47.8%) of the respondents were sure that the in charge of IT was tasked with the daily backup of the information in the hospitals servers while 52.2% of them had no knowledge hence opted for the response partially addressed.

Table 7 Knowledge of reliable information backup Source: Author's Data (2014)

knowledge of reliable information backup

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	fully addressed	7	15.2	15.2	15.2
	Addressed	15	32.6	32.6	47.8
	partially addressed	24	52.2	52.2	100.0
	Total	46	100.0	100.0	

A careful interrogation with the system administrators on issues of managing security efficiently and effectively in a systematic manner, presence of backup facilities and disaster recovery plans revealed the following. CSCH reported the most inefficient (risk rating 9) approach of managing information security incidents consistent with applicable policies while JOOTRH and KCH risk ratings stood at medium (6). This includes information about incident reporting, health facilities response, operations relocation, collection of evidence and system recovery.

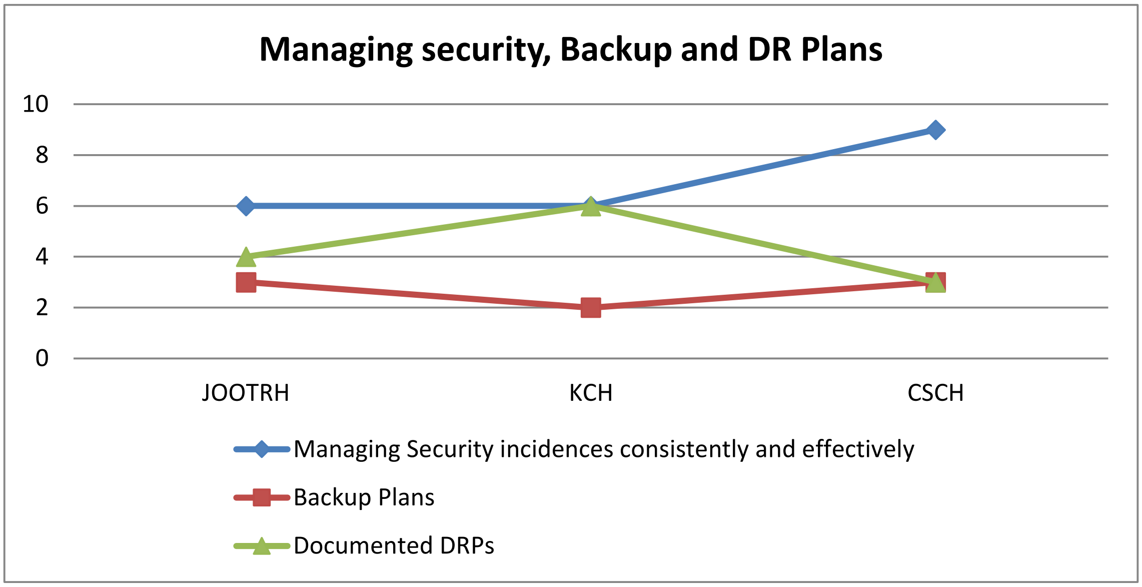


Figure 7 Managing security, Backups and Disaster recovery plans Source: Author's Data (2014)

All the three heath facilities have systems in place to backup critical data and IT system installations hence reported low risk rating as follows JOOTRH (3), KCH (2) and CSCH (3). The most efficient disaster recovery plans was reported at KCH risk rating 6 (medium) while JOOTRH risk ratings 4 (medium) and CSCH risk rating 3 (low).

The following can be deduced as overal observations on this category:

a. Information involved in electronic messaging is compromised.
b. Inability of managing security incidences consistently and effectively.
c. Lack of documented disaster recovery plans inhibits the recovery of information systems.

4.3 Reliability Analysis for the variables

The scale for measuring the risk management security was made up of sixteen variables. In order to assess whether the twelve variables made a reliable scale, the Cronbach's alpha was computed. In an initial reliability analysis, the value of alpha for the twelve variables was .629. Subsequent deletions and further inclusions of some variables after the pretest exercise increased the value of alpha to .789 .The final value of alpha was .856 indicating that the remaining twelve variables form a scale with good internal consistency reliability. Table 18 below shows the final reliability statistics while table 19 gives a description of the twelve variables used in the reliability analysis.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.825	.823	12

Table 8: Final reliability statistics

	Item Statistics			
	Variable	Mean	Std. Deviation	N
T1	designated in charge of computer and information security	2.91	0.784	46
T2	undertaken a structured risk assessment of information security	3.07	1.181	46
T3	presence of documented policies and procedures for managing InfoSec	3.74	0.999	46
T4	well established and monitored authorized access to health information	2.87	1.166	46
T5	documented and tested plans for business continuity and information recovery	3.48	1.243	46
T6	processes for safe and proper use the internet and email in conformity with hospital policies and procedures for information security	3.93	0.827	46
T7	knowledge of reliable information backup	2.37	0.741	46
T8	reliable protection against malware and viruses	3.17	1.18	46
T9	reliable computer network perimeter controls	3.3	0.963	46
T10	safe and proper use mobile electronic devices to manage information security	3.72	1.148	46
T11	are you in charge of the physical security of hardware n software with a view to protect information security	2.63	0.645	46

T12	reliable system for secure sharing of confidential information	3.35	0.875	46

Table 9: Item statistics description of the twelve variables

4.4 Challenges encountered in the implementation of FUNSOFT

Though this subject was not originally itemized as part of the data to be collected, it was established during pretesting that other than security issues around the FUNSOFT platform, many of its daily users had challenges that they felt prudent to enlist them as a concern. The following were the main challenges encountered by the FUNSOFT users;

a. The accountants reported that the system had many errors which none of them understood including the system admin hence there is over reliance on the IT vendors for the successful implementation of the system

b. The system development did not include the users in the design and development stages hence the system has technical terms that are not understood by the routine system users

c. All the three facilities had concerns with the speeds of the system operation though JOOTRH installed an extra server and since then the speeds have slightly improved

d. Regular nearing daily breakdowns of the system. Clinical officers have adopted a silent position that when the system is down service delivery is halted until it comes back. This greatly affects the patients who need this critical service irrespective of the state of the Funsoft system.

e. Resistance to change by some of the users who have made the implementation of the system a nightmare

f. The dental platform is completely not user friendly as most of the components they use are not installed in the application.

g. Few desktops. Most departments have one computer assigned to them hence if there are five doctors for example in the dental unit at work they have to cue to use the system

h. The system has issues with operability between the pharmacy and the dental unit

i. The computers security is attached to the user as a result of insecurity incidences and this makes the assigned users not to be willing to share the resource even in their absence

j. All interns sharing one password

k. There existed a culture of "assisting (corruption)" patients before the system was implemented and this has been discarded.

l. At KCH there are complications with inpatient ID and outpatient ID as the system is only operational at the outpatient facility. This forces one user to have two IDs

m. No clear documentation on the system

CONCLUSION

There is need to identify key personnel who will acquire necessary skills in management of information security and ICT management for the HMIS platform from the inception of the project. These key personnel should be retained to make sure that their knowledge has been imparted to other personnel in the health facility and county at large.

REFERENCES

Alshaikh., Ahmad., Maynard & Chang., (2014). *Towards a Taxonomy of Information Security Management Practices in Organizations*

Bertino E & Sandhu R., (2005). *Database Security-Concepts, Approaches, and Challenges*. IEEE Trans. Dependable Security Computing. 2(1): 2-19

Bowen, Hash & Wilson., (2006). *Information Security Handbook*: A Guide for Managers, Recommendations of the National Institute of Standards and Technology, NIST SP 800-100, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg.

Brian Cusack., (2010). *Objectives Alignment: Reworking IS Security for eBusiness Enterprises,* Americas Conference on Information Systems (AMCIS), Association for Information Systems

Busch, Rebecca S., (2008). Electronic Health Records: An Audit and Internal Control Guide.

Caballero & Alberto., (2010). *Information and Computer Security Handbook.* Morgan Kaufmann Publications, Elsevier.

Coyne & Edward J., (2007). *Role Engineering for Enterprise Security Management*, Norwood, MA, USA: Artech House.

Creswell, J. W. (2007). Qualitative Inquiry and Research Design; Choosing among five approaches. London, New Delhi: Sage Publications, Inc.

Evans Wheeler., (2012). *Security Risk Management: Building an Information Security Risk Management Program from the Ground Up*

Ferraiolo & David F., (2007). *Role-Based Access Control* (2nd Edition).Norwood, MA, USA: Artech House

Georg Disterer.,(2011). ISO/IEC 27000, 27001, 27002. *Information Security Management*, University of Applied Sciences and Arts, Hannover, Germany

George (2003). *Information technology security handbook.* The International Bank for Reconstruction and Development / The World Bank

INSEAD, World Economic Forum. (2013). *The Global Information Technology Report 2013.* Geneva: World Economic Forum.

ISACA. (2006). *Information Systems Control Journal.* USA

Ken Scarfan & Paul Hoffman., (2009). *Guidelines on firewalls and firewall policy*. NIST SP 800-40 , Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology. Gaithersburg

Kevin Stine, Rich Kissel, William C. Barker, Jim Fahlsing & Jessica Gulick., (2008). *Guide for Mapping Types of Information and Information Systems to Security Categories*, NIST SP 800-60, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg, MD 20899-8930

Kim JH & Kim HE.,(1999). *Surveying the attitude of social groups towards privacy, confidentiality and security of health information*. J Korean Soc Med Inform. 63–76.

Laborde , Nasser , Grasset , Barrère , Benzekri.,(2005). *A Formal Approach for the Evaluation of Network Security Mechanisms Based on RBAC Policies.* Proceedings of the 2nd International Workshop on Security Issues with Petri Nets and other Computational Models (WISP 2004) Pages 117–142. University Paul Sabatier, Toulouse, France.

Lichtenstein & Swatman., (2010). *Effective Management and Policy in e- Business Security*, 14th Bled Electronic Commerce conference

Mario Spremi.,(2012). *Corporate IT Risk Management Model*: a Holistic view at Managing Information System Security Risks. Faculty of Economics and Business Zagreb, University of Zagreb Kennedy's sq 6, 10000 Zagreb

Matt Smith., (2013). *Hacker Proof:* You're Guide to PC Security

McClure, Scamray & Kurtz., (2009). *Hacking Exposed. Network Security Secrets and solutions, 4th edition*. Tata McGraw-Hill

Michael E. Whitman and Herbert J. Mattord (2009). *Principles of Information Security, 5th Edition*, Michael J. Coles College of Business, Kennesaw State University ISBN-13: 9781285448367

Mishra D., (2013). *A Study on ID-based Authentication Schemes for Telecare Medical Information* SystemarXiv

Muaz & Jalil.,(2013). *Practical Guidelines for conducting research.* Summarizing good research practice in line with the DCED Standard

Murrey & Frenk., (2000). *A framework for assessing the performance of health systems*. World health organization. Geneva

NIST SP 800-37, (2010). *Guide for applying risk management framework to federal information systems. A security life cycle approach*, Joint task force transformation initiative, Recommendations of the National Institute of Standards and Technology, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg.

Njenga & Brown., (2010). *The Case for Improvisation in Information Security Risk Management*. E-Government, E-Services and Global Processes, 220-230

Nocco, B & danStulz, R., (2006). *Enterprise Risk Management: Theory and Practice,* Journal of Applied Corporate Finance, vol.18, no.4.

OHSAS 18001 (2007). *Guidelines for the implementation of Occupational Health and Safety Management Systems* (OHS-MS) 18001

Olivier, M. S., (2009). *Information technology research: A practical guide for computer science and informatics* (3rd ed.). Pretoria: Van Shaik.

Oxford dictionary of computing., (2006). Oxford university press

Peppard, & Ward.,(2004). *Beyond strategic information systems. Towards an IS capability*, Journal of Strategic Information Systems, 167-194.

Purser & Steve.,(2011). *A Practical Guide to Managing Information Security*. Norwood, MA, USA: Artech House

Quirchmayr , Slay, Koronios & Darzanos., (2011). *A business Process Engineering Based Approach Towards Incorporating Security in the Design of Global Information Systems*, 7th Pacific Asia Conference on Information Systems. Handbook of Electronic Security and Digital Forensics. World Scientific International Journal of Electronic Security and Digital Forensics 1 (1), 76-88.

Ramiller & Swanson., (2003). Organizing Visions for Information Technology and the Information Systems executive response. *Jornal of Management Information Systems, 20*(1), 13-50.

Saunders, Lewis & Thornhill.,(2009). *Reasearch methods for business students* (5th ed.). England: Pearson Education Limited.

Slade & Rob (2006). *Dictionary of Information Security*, Rockland, MA, USA, Syngress Publishing

Sokratis & Katsicas. (2009). *Information and Computer Security Handbook.* Morgan Kaufmann Publications, Elsevier.

Spremic.,(2009). *IT Governance Mechanisms in Managing IT Business Value*, WSEAS Transactions on Information Science and Applications, Issue 6, Volume 6, 906-915.

Stephan Schmidt & Sahin Albayrak (2010). 10th International Conference on Intelligent Systems Design and Applications.

Steve Elky, (2006). *An Introduction to Information System Risk Management.* SANS Institute, InfoSec Reading Room - 2007 - pp. 1-18 - SANS Institute - 2007 - http://www.sans.org

Stoneburner, Goguen, & Feringa., (2009). *Risk Management Guide for Information Technology Systems.* Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology. Gaithersburg

Swanson & Guttman.,(1996). NIST, *Generally Accepted Principles and Practices for Securing Information Technology System*

Thomas, Tryfonas & Owen., (2010). *Is There a Case for Liability of Software Vendors?* Malicious Software and System Damages. Proceedings of the 6th European Conference on Information Warfare & Security Technical Standard Risk Taxonomy the African Journal of Information and Communication 13, 42-61.

Venkatesh, Brown & Bala.,(2013). *Bridging the qualitative–quantitative divide*: guidelines for conducting mixed methods.

Webb, Maynard, Ahmad & Shanks., (2013). *Towards an Intelligence-Driven Information Security Risk Management Process for Organizations*

WHO., (2008). *Framework and Standards for Country Health Information Systems.* Health Metrics Network. World Health Organization, Geneva, Switzerland