Assessment Of Ict Disaster Recovery And Preparedness Among Health Research Institutions In Kisumu County, Kenya

Collins Awiti[1], Dr. Silvance O. Abeka[2], Dr. Samuel Liyala[3]
School Of Informatics and Innovative Systems
Jaramogi Oginga Odinga University of Science & Technology
colly_awiti@yahoo.com[1], silvancea@gmail.com[2],sliyala@yahoo.com[3]

Abstract— Research organizations utilize information technology to generate process and transmit both sensitive and vital data that is critical in development of drugs, vaccines and health policy. Despite the role ICT plays in this research organization little has been done to assess the level of preparedness and capacity to mount effective recovery mechanism in case of an ICT disaster within these organizations. Therefore, the purpose of this study is to assess how prepared the health research organizations are in case of ICT related disaster. The study objective will be to identify existence of ICT infrastructure, to assess the existing of ICT disaster recovery plan on disaster response preparedness and to examine the influence of ICT disaster recovery policies on disaster response in health research organizations in Kisumu County. This study intended to identify existence of IT infrastructure in relation to recovery among ICT staff and users in health research organizations in Kisumu County. Survey design will be adopted and a saturated sampling method will be deployed in selecting a sample population of 25 respondents. Data were collected through structured questionnaire. The validity and reliability of the research instrument was also be tested. The data was analyzed through descriptive statistics (mean, standard deviation); also, inferential statistics (regression) was used to analyze data. The research key findings revealed that there is adequate infrastructure across the organizations. However, not adopting cloud computing technology in enhancing disaster recovery service had the lowest mean rank of (3.48) on a scale of 1 (Strongly Disagree) to 5(Strongly Agree). Which indicates that most organizations have not adopted cloud computing technology as part of disaster recovery services. The research findings would be valuable to the Ministry of Health, Health Research Institutions and the public sector, policy makers as it will give them basis for embracing disaster management.

Index Terms— *Disaster Awareness, Disaster Preparedness, Disaster Recovery, ICT, Health Research Institutions*.

1.0 INTRODUCTION

Disaster can occur anytime and anywhere whether manmade or natural the situation can be disastrous. Disasters have negatively affected humans since the dawn of our existence. In response individuals and societies alike have made many attempts to decrease their expose to the consequences of these disasters, developing measures to address initial impact, regardless of the approach adopted all these efforts have the same goal (Coppola, 20011:2).
The concept disaster is defined as disruption of the functioning of an organization, community, and society causing widespread human, material, economic, technological or environmental losses, which exceed the ability of the affected organizations and society to cope using its own resources (Paton and Johnston (2001). This is further supported by Alexander (1997) who defined disasters as events that displace the structural, technological, economic, organizational, cultural and spiritual well-being of communities by destroying their means of existence. Disaster could be either human-induced, technological errors or natural occurrences. They are natural if they just happen without being induced by humans like tsunamis, volcanoes, earthquakes, storms and floods.

The effects of disasters on human life and economic activities necessitates that a disaster recovery and preparedness plans be in place. In this context, disaster recovery involves a set of policies and procedures put in place to enable continuation of vital information technology infrastructure and systems following a man-made or natural disaster. On the other hand, disaster preparedness refers to activities and measures taken in advance to ensure effective response to the impact of disasters, including the issuance of timely and effective early warnings and the temporary removal of people and property from a threatened location (ISDR, 2002). It also entails putting measures in place technologically to be able to bounce back when a disaster occurs and minimize the down time (ISDR, 2002).

Worldwide many organizations both government and private have adopted the use of IT in service provision. Adoption of IT in this case is aimed at improving efficiency in operations thus saving costs and maximizing profits. The widespread adoption of ICT simultaneously calls for adequate preparation and mitigation against ICT related disasters. Several IT disasters have been reported in the world. The unique one being the President Obama www.healthcare.gov website, which could not launch on October 2013 after a lot of publicity and funds being spent to set it up. US citizens seeking health insurance were denied access to the website and had to resort to phone lines and posting mails. Lack of testing and disaster preparedness was flagged as the key reason behind the failure leaving Obama health care officials looking unprepared and incompetent.

In Kenya a typical example of an IT related disaster was when

the Independent Election and Boundaries Commission (IEBC) of Kenya had their electronic voting system interfered with and they were unable to recover and continue with their business as usual reference. As reported in the East African Standard Wednesday, 31st July 2013, this is a typical scenario of lack of disaster preparedness and the impact to the whole nation was just unbearable.

Information technology is integral in medical research in Kenya which has seen a growth in number of organizations conducting health research from one in 1976 to over 10 in 2006 (Patel, 2006). According to Kenya Medical Research institute (KEMRI) which is the regulatory body guiding medical research in Kenya there are numerous ongoing research studies, surveillance, health systems research and support programs at their centers in Kisumu. The research revolve around studying efficacy of drugs, emergence of drugs and vector resistance, immunology, climate and human health, malaria vaccine trials, HIV/AIDS and its impact on the community, HIV interactions with other infectious diseases such as Tuberculosis. This kind of excellent work has attracted both local and international organizations to invest more on health research in Kenya. Some of the notable funders include Novartis, Glaxo Smith Kline (GSK), Melinda, and Bill Gates foundation that work in close relationship with local organizations like CDC, Walter Reed Project, ICAP, and ICIPE amongst others.

With all this effort being put on research it is paramount that the data collected has to be accurate, has to have integrity, secure and available all of the time. This requires creation of a system of disaster preparedness across all the centers conducting research. The rise in number of health research organizations is associated with increased use in Information Technology in these organizations. However, it has not been documented whether these organizations have incorporated disaster preparedness while adopting the use of Information Technology. While some of the organizations might have an ICT disaster plan in place it is not clearly known how frequently systems and staff are updated to be able to address an ICT related disaster. Therefore, using a number of large and medium health research organizations this study seeks to assess how prepared the health research organizations are in case of ICT related disaster.

2.0 LITERATURE REVIEW

2.1 ICT infrastructure in relation to disaster

ICT Infrastructure put in place will really determine a lot about how an organization will bounce back or continue with its normal operations whenever a disaster occurs. Infrastructure would generally include hardware and facilities put in place. These might include off site stations, back up mechanism, recovery procedures amongst others.
According to Mnjama and Wamukoya (2007) on a research done about e-government and records management in Botswana, They argue that, while many governments have systems and procedures for managing information assets there is lack of a proper mechanism and adequate infrastructure to safeguard against a disaster and a disruption that could bring down an organization to a stand. The previous study was done in Botswana, while the present study will focus on existence of ICT infrastructure in relation to disaster response in health research organizations in Kisumu County, Kenya.

According to Haeke (2011), some of the ICT facilities that an organization can use include:
Onsite Storage: Onsite storage usually refers to a location on the site of the computer center that is used to store information locally. Onsite storage containers are available that allow computer cartridges and tapes or backup media to be stored in a reasonably protected environment in the building. Onsite storage containers are designed and rated for fire, moisture, and pressure resistance. These containers are not fireproof in most cases, but they are indeed fire rated. A fireproof container should be guaranteed to withstand damage regardless of the type of fire or temperature, whereas fire ratings specify that a container can protect its contents for a specific amount of time in a given situation.

Offsite Storage Offsite storage refers to a location away from the computer center where paper copies and backup media are kept. Offsite storage can involve something as simple as keeping a copy of backup media at a remote office, or it can be as complicated as a nuclear-hardened, high-security storage facility. The various Types of back ups are as follows:

Full Backup A full backup is a complete, comprehensive backup of all files on a disk or server. The full backup is current only at the time it is performed. Once a full backup is made, you have a complete archive of the system at that point in time. A system should not be in use while it undergoes a full backup because some files may not be backed up. Once the system goes back into operation, the backup is no longer current.

Incremental Backup An incremental backup is a partial backup that stores only the information that has been changed since the last full or the last incremental backup. If a full backup was performed on a Sunday night, an incremental backup done on Monday night would contain only the information that changed since Sunday night. Such a backup is typically considerably smaller than a full backup. Each incremental backup must be retained until a full backup can be performed. Incremental backups are usually the fastest backups to perform on most systems, and each incremental backup tape is relatively small.

A differential backup is similar in function to an incremental backup, but it backs up any files that have been altered since the last full backup; it makes duplicate copies of files that have not changed since the last differential backup. If a full backup were performed on Sunday night, a differential backup performed on Monday night would capture the information that was changed on Monday. A differential backup completed on Tuesday night would record the changes in any files from Monday and any changes in files on Tuesday.

A study carried out by Srinivas, Seetha Ramayya, and Venkatesh (2013) in India on disaster recovery as a service of cloud computing. The finding showed that it was low cost service when compared to traditional disaster recovery. It was flexible in replicating physically or virtually. It provided application consistent recovery for some working applications like SQL server. It had pre-built options for virtual recovery environments including security, network connectivity and server failover when continuously replication among servers. When disaster occurs, we can take backup and we can run our applications on service provided by disaster recovery until we get backup to primary site. Disaster recovery as a service to replicate critical servers and data centre infrastructure in cloud. Disaster recoveries as a service is free or pay on use offer. When incompatibilities occur due to software changes, then breaking of DRaaS in cloud may occur. Three models define the architecture of DRaaS. From Cloud: when the primary application or data is in cloud and backup or recovery site is in private data centre. In cloud: when both primary site and recovery site are in cloud. To cloud: when the application is in primary data centre and backup or recovery site is in cloud. To test the recovery processes sandboxes are used and they test without disrupting running application. It is only accessible to only system administrator. Solutions are pre-packaged services that provide a standard DR Failover to a cloud environment that you can buy on a pay-per-use basis with varying rates based upon your recovery point objective (RPO) and recovery time objective (RTO).

Further, Jadeja and Modi (2012) established that in case of disasters, an offsite backup is always helpful. Keeping crucial data backed up using cloud storage services is the need of the hour for most of the organizations. In addition, cloud storage services not only keep your data off site, but they also ensure that they have systems in place for disaster recovery. Jadeja and Modi (2012) also asserted that cloud computing provides lower outages, thus providing uninterrupted services to the user and the cloud computing systems are much more dependable compared to the infrastructure installed on the organization.

Another study by Kiblin (2011) on how to use cloud computing for disaster recovery showed that disaster recovery in the cloud is offering companies more options to restore data quickly and effectively than with a traditional disaster recovery model. In the past, companies used manual tape backups, which are cumbersome and unreliable, and even disk backups have to be stored somewhere safe, either onsite or ideally, remotely. Cloud disaster recovery solutions offer hot, warm and cold site options, where a company can choose the how often and in how many locations data is backed up.

2.2 ICT disaster recovery plan on disaster response preparedness

A disaster recovery plan (DRP) is a documented process or set of procedures to recover and protect a business ICT infrastructure in the event of a disaster (Bill,2012). Such a plan, ordinarily documented in written form, specifies procedures an organization is to follow in the event of a disaster. It is "a comprehensive statement of consistent actions to be taken before, during and after a disaster.

According to Wold (1997), the entire process involved in developing a Disaster Recovery Plan consists of 10 steps: this include: Step 1: Obtaining top management commitment: For a disaster recovery plan to be successful, the central responsibility for the plan must reside on top management. Management is responsible for coordinating the disaster recovery plan and ensuring its effectiveness within the organization. It is also responsible for allocating adequate time and resources required in the development of an effective plan. Resources that management must allocate include both financial considerations and the effort of all personnel involved.

Step 2: Establishing a planning committee: A planning committee is appointed to oversee the development and implementation of the plan. The planning committee includes representatives from all functional areas of the organization. Key committee members customarily include the operations manager and the data processing manager. The committee also defines the scope of the plan.

Step 3: Performing a risk assessment: The planning committee prepares a risk analysis and business impact analysis (BIA) that includes a range of possible disasters, including natural, technical and human threats. Each functional area of the organization is analyzed to determine the potential consequence and impact associated with several disaster scenarios. The risk assessment process also evaluates the safety of critical documents and vital records. Traditionally, fire has posed the greatest threat to an organization. Intentional human destruction, however, should also be considered. A thorough plan provides for the "worst case" situation: destruction of the main building. It is important to assess the impacts and consequences resulting from loss of information and services. The planning committee also analyzes the costs related to minimizing the potential exposures.

Step 4: Establishing priorities for processing and operations: At this point, the critical needs of each department within the organization are evaluated in order to prioritize them. Establishing priorities is important because no organization possesses infinite resources and criteria must be set as to where to allocate resources first. Some of the areas often reviewed during the prioritization process are functional operations, key personnel and their functions, information flow, processing systems used, services provided, existing documentation, historical records, and the department's policies and procedures. Processing and operations are analyzed to determine the maximum amount of time that the department and organization can operate without each critical system. This will later be mapped into the recovery time objective. A critical system is defined as that which is part of a system or procedure necessary to continue operations should a department, computer center, main facility or a combination of these be destroyed or

become inaccessible. A method used to determine the critical needs of a department is to document all the functions performed by each department. Once the primary functions have been identified, the operations and processes are then ranked in order of priority: essential, important and non-essential.

Step 5: Determining recovery strategies: During this phase, the most practical alternatives for processing in case of a disaster are researched and evaluated. All aspects of the organization are considered, including physical facilities, computer hardware and software, communications links, data files and databases, customer services provided user operations, the overall management information systems (MIS) structure, end-user systems, and any other processing operations. Alternatives, dependent upon the evaluation of the computer function, may include hot sites, warm sites, cold sites, reciprocal agreements, the provision of more than one data center, the installation and deployment of multiple computer system, duplication of service center, consortium arrangements, lease of equipment, and any combinations of the above.
Written agreements for the specific recovery alternatives selected are prepared, specifying contract duration, termination conditions, system testing, cost, any special security procedures, procedure for the notification of system changes, hours of operation, the specific hardware and other equipment required for processing, personnel requirements, definition of the circumstances constituting an emergency, process to negotiate service extensions, guarantee of compatibility, availability, non-mainframe resource requirements, priorities, and other contractual issues.

Step 6: Collecting data: In this phase, data collection takes place. Among the recommended data, gathering materials and documentation often included are various lists (employee backup position listing, critical telephone numbers list, master call list, master vendor list, notification checklist). Inventories (communications equipment, documentation, office equipment, forms, insurance policies, workgroup and data center computer hardware, microcomputer hardware and software, office supply, off-site storage location equipment, telephones, etc.), distribution register, software and data files back-up/retention schedules, temporary location specifications, any other such other lists, materials, inventories and documentation. Pre-formatted forms are often used to facilitate the data gathering process.

Step 7: Organizing and documenting a written plan: Next, an outline of the plan's contents is prepared to guide the development of the detailed procedures. Top management reviews and approves the proposed plan. The outline can ultimately be used for the table of contents after final revision. Other four benefits of this approach are that (1) it helps to organize the detailed procedures, (2) identifies all major steps before the actual writing process begins, (3) identifies redundant procedures that only need to be written once, and (4) provides a road map for developing the procedures. It is often considered best practice to develop a standard format for the disaster recovery plan to facilitate the writing of detailed procedures and the documentation of other information to be included in the plan later. This helps ensure that the disaster plan follows a consistent format and allows for its ongoing future maintenance. Standardization is also important if more than one person is involved in writing the procedures. It is during this phase that the actual written plan is developed in its entirety, including all detailed procedures to be used before, during, and after a disaster. The procedures include methods for maintaining and updating the plan to reflect any significant internal, external or systems changes. The procedures allow for a regular review of the plan by key personnel within the organization. The disaster recovery plan is structured using a team approach. Specific responsibilities are assigned to the appropriate team for each functional area of the organization. Teams responsible for administrative functions, facilities, logistics, user support, computer backup, restoration and other important areas in the organization are identified. The structure of the contingency organization may not be the same as the existing organization chart. The contingency organization is usually structured with teams responsible for major functional areas such as administrative functions, facilities, logistics, user support, computer backup, restoration, and any other important area.
The management team is especially important because it coordinates the recovery process. The team assesses the disaster, activates the recovery plan, and contacts team managers. The management team also oversees documents and monitors the recovery process. It is helpful when management team members are the final decision-makers in setting priorities, policies and procedures. Each team has specific responsibilities that are completed to ensure successful execution of the plan. The teams have an assigned manager and an alternate in case the team manager is not available. Other team members may also have specific assignments where possible.

Step 8: Developing testing criteria and procedures: Best practices dictate that DR plans be thoroughly tested and evaluated on a regular basis (at least annually). Thorough DR plans include documentation with the procedures for testing the plan. The tests will provide the organization with the assurance that all necessary steps are included in the plan. Other reasons for testing include:

- Determining the feasibility and compatibility of back-up facilities and procedures.
- Identifying areas in the plans that need modification.
- Providing training to the team managers and team members.
- Demonstrating the ability of the organization to recover.
- Providing motivation for maintaining and updating the disaster recovery plan.

Step 9: Testing the plan: After testing procedures have been completed, an initial dry run of the plan is performed by conducting a structured walk-through test. The test will provide additional information regarding any further steps that may need to be included, changes in procedures that are not effective, and other appropriate adjustments. These may not be-

come evident unless an actual dry-run test is performed. The plan is subsequently updated to correct any problems identified during the test. Initially, testing of the plan is done in sections and after normal business hours to minimize disruptions to the overall operations of the organization. As the plan is further, polished, future tests occur during normal business hours.
Types of tests include checklist tests, simulation tests, parallel tests, and full interruption tests.

Step 10: Obtaining plan approval: Once the disaster recovery plan has been written and tested, the plan is then submitted to management for approval. It is top management's ultimate responsibility that the organization has a documented and tested plan. Management is responsible for (1) establishing the policies, procedures and responsibilities for comprehensive contingency planning, and (2) reviewing and approving the contingency plan annually, documenting such reviews in writing.
Organizations that receive information processing from service bureaus will, in addition, also need to (1) evaluate the adequacy of contingency plans for its service bureau, and (2) ensure that its contingency plan is compatible with its service bureau's plan.

Boyd and Juhola, (2009) indicate that capacity building provides an opportunity to understand strengths, weaknesses, threats and opportunities towards a resilient future through identification of broader issues around sustainable development of a particular program, project or process, including their unique cultural, social, and ecological characteristics.
Moreover, ICT can play a significant role in highlighting risk areas, vulnerabilities and potentially affected populations by producing geographically referenced analysis through, for example, a geographic information system (GIS). The importance of timely disaster warning in mitigating negative impacts can never be underestimated. A warning can be defined as the communication of information about a hazard or threat to a population at risk, in order for them to take appropriate actions to mitigate any potentially negative impacts on themselves, those in their care and their property (Samarajiva et al., 2005)

3.0 RESEARCH METHODOLOGY

3.1 Research Design
A descriptive survey research design was adopted for this research. The design was deemed appropriate as it had the advantage of exploring the current level of ICT disaster preparedness and recovery in health research organizations in Kisumu County; thereby revealing summarised statistics by showing responses to all possible questionnaire items that lead to identifying needed changes.

3.2 Study area
Kisumu town is the third largest city in Kenya with a population of approximately 345,312. Kisumu Town is the administrative headquarters of the Kisumu County. Kisumu town has developed progressively from a railway terminus and internal port in 1901, to become the leading commercial/trading, industrial, communication and administrative centre in the Lake Victoria basin, an area that traverses three provinces of Nyanza, Western and western Rift Valley. The researcher found the study area to be suitable because it host major health research organizations in the country. These include The Walter Reed Project, Center for Disease Control, ICAP, FACES, Nyanza Reproductive, IMPACT Research and Development.

3.3 Target population
The study population was be 25 staffs from the ICT department from the eight Health Research organizations within Kisumu County. The target population comprised of five Chiefs of ICT, 6 network administrators, 5 system administrators and 9 user support technicians for the targeted health research organizations in Kisumu County. Study population means all elements who share one or more common quality in a special geographical scale (Creswell, 2014). It is a complete set of individuals, cases or objects with some common characteristics that differentiate it from other population (Kothari, 2012).

3.4 Sampling Techniques and Sample Size
The study adopted saturated sampling technique to select the 25 out of 25 respondents. This is because saturated sampling technique allows the researcher to have all the study population covered.

3.5 Research Instrument
This research project employed the use of self administered close-ended structured questionnaire. This was guided by the vast nature of the data that was to be collected, the time available and the objectives of the study. Data collection instrument was pretested to determine their validity and reliability. The questions were formulated by the researcher and tested to ensure their conformity. Face Validity and Content Validity approach was used for the study. In content validity, the data instrument was tested in a pilot study to establish if it contains all possible items that was to be used in measuring the concepts (Rugg & Petre, 2007). This confirmed that there were enough items and questions in instrument covering the study topic. The researcher used the expert judgment method to determine Face validity. A copy of the questionnaire was given to the supervisor to check if it represented all the objectives of the study. Test-retest reliability was used for this study (Sekaran & Bougie, 2010). The test-retest was administered to staff and students of the universities and the same test was also administered after 2 weeks. The scores from time 1 and time 2 were then correlated in order to evaluate the test for stability of time. To measure the degree to which the questionnaires will yield consistent result or data, the researcher computed the Cronbach's coefficient Alpha technique to establish how items correlate amongst themselves to determine reliability.

Table 1: Cronbach's alpha reliability test value

Reliability Statistics

Cronbach's Alpha	N of Items
.843	37

This meant all constructs were internally consistent and measured the same content of the construct. The findings thus show that the questionnaire used in the study was reliable and the results of the questionnaire can be relied on as the alpha values were above 0.70.

4.0 RESULTS

This section presents the results obtained from this study. 25 ICT accepted to be interviewed and completed the questionnaire representing 100% response rate.

Table 2: Respondents Characteristics

Characteristics	Categories	n	%
Gender	Female	7	28.0
	Male	18	72.0
Duration of work	Less than 2 years	7	28.0
	2-5years	7	28.0
	Over5 years	11	44.0
Level of Education	Diploma	3	12.0
	Degree	15	60.0
	Post Grad	7	28.0
Number of Employee's supported	20-50	12	48.0
	51-100	4	16.0
	>100	9	36.0

Table 2 shows the demographic characteristics of respondents and number of employees supported by ICT department. More than two –thirds of respondents were male(n=18,72%) as compared to female(n=7,28%). More than half of respondents had worked in their current organization for less than 5 years. In terms of education, 60%(n=15) of respondents have attained Bachelor's degree level of education as compared to 12%(n=3) with diploma and 28%(n=7) with post-graduate level of education. In terms of employee supported, 48%(n=12) indicated they supported less than 50 employees while 36%(n=9) indicated they supported more than 100 employees.

4.1: To identify existence of ICT infrastructure in relation to disaster response in health research organizations in Kisumu County.

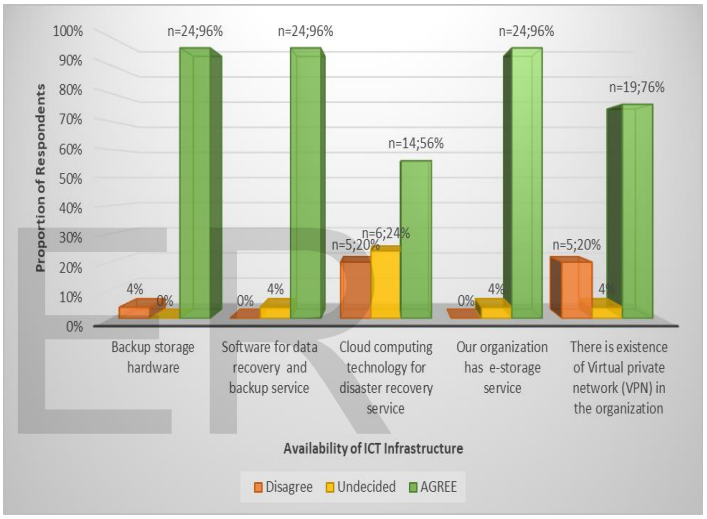

Figure 1: Availability of ICT Infrastructure

Figure 1 above shows the availability of ICT infrastructure across different organizations as indicated by respondents. Across the organizations, there was availability of back-up storage hardware (n=24;96%), there was software for data recovery and back-up service(n=24;96%) and there exists and e-storage service(n=24;96%). The least available infrastructure is cloud computing (n=14;56%) for disaster recovery services. On overall most organization had adequate infrastructure to support data recovery incase of ICT related disaster.

This study has observed that most health research organizations have hardware's and software's that can support recovery following ICT related disasters. However, this study has also observed that most organizations have not adopted modern disaster recovery measures such as cloud computing and use of Virtual Private Network. These findings suggest that most organizations can suffer irreparable damage should a disaster that affects ICT system occur. Such risks can occur since most organization relay on hard drives for back-up such that any loss or damage to the hard drives can affect ability of those organizations to recover from disasters. In concurring

with the findings of this study Mnjama and Wamukoya (2007) indicated that while many governments have systems and procedures for managing information assets there is lack of a proper mechanism and adequate infrastructure to safeguard against a disaster and a disruption that could bring down an organization. In concurring with finding of this study Srinivas et al (2013) indicated that cloud computing is a low cost service when compared to traditional disaster recovery plan. They highlighted that cloud computing is flexible in replicating physically or virtually as it provides a consistent recovery for some working applications like SQL server.

Not adopting cloud computing technology in enhancing disaster recovery service had the lowest mean rank of which indicates that most organizations have not adopted cloud computing technology as part of disaster recovery services. As observed by Kiblin (2011) cloud computing offers organizations more options to restore data quickly and effectively than with a traditional disaster recovery model. He argued that while use of manual tape backup is cumbersome and unreliable while cloud disaster recovery solutions offer hot, warm and cold site options, where a company can choose the how often and in how many locations data is backed up.

4.2: ICT disaster recovery plan on disaster response preparedness in health research organizations in Kisumu County.

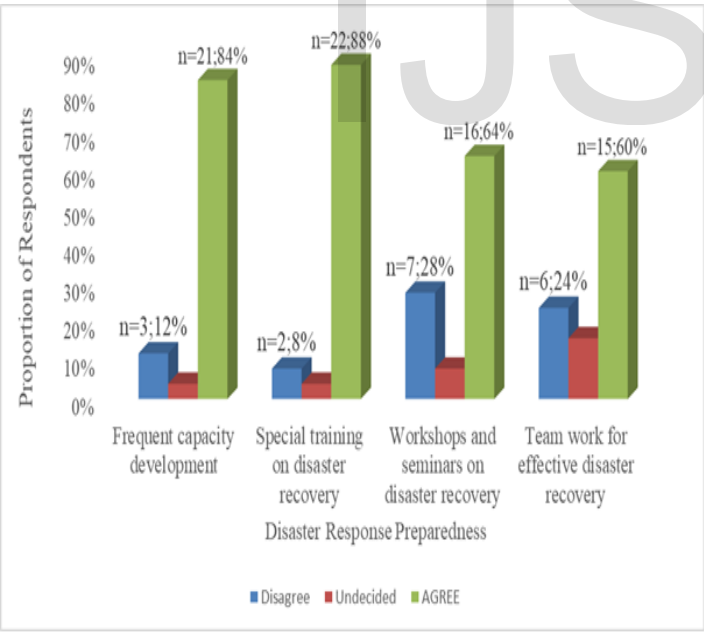

Figure 2: Disaster response preparedness

Figure 2 shows elements of disaster preparedness across organization as indicated by respondents. Most respondents at 88%(n=22) indicated they undergo special training on ICT-disaster recovery while 84%(n=21) indicated they are provided with frequent capacity development on ICT-disaster recovery. On the other hand 64%(n=16) of respondents indicated they have had opportunity to attend workshops and seminars on ICT disaster recovery. While 60%(n=15) indicated there is teamwork across organization in promoting effective disaster recovery.

Boyd and Juhola, (2009) indicate that capacity building provides an opportunity to understand strengths, weaknesses, threats and opportunities towards a resilient future through identification of broader issues around sustainable development of a particular program, project or process, including their unique cultural, social, and ecological characteristics. This capacity building is lacking in most of the institutions we surveyed. More trainings and workshops which are vital to equip the recovery team with skills and expose them.
According to Wold (1997), the entire process involved in developing a Disaster Recovery Plan consists of 10 steps but the results realized that some steps were skipped either by omission or commission. These steps must be all followed for the success of the plan.

The study has observed that most of the organization`s recovery plans are not well implemented. They are well formulated but not tested properly to confirm if the plans can work. The research has also revealed that there is need for the departments to be involved in the process of developing the recovery plans. Frequent drills should be organized.

5.0 RECOMMENDATIONS AND FUTURE RESEARCH

This study makes significant contributions to knowledge in relation to disaster management in health research organizations specifically ICT related disaster. In the light of these findings, several recommendations are made which may be useful for health research organizations and other related authorities. Institutions should have policies and procedures in place for effective disaster management and response. The organizations also lack team work and the inter relationship between the various departments should be improved since they need each other. Also of notable concern was the lack of commitment in support from the top most management is supporting IT departments to enable them function optimally. This is necessary since all these activities have financial implications.
It is suggested that more research should be done on the development of enhance frameworks for disaster preparedness and recovery in health research organizations. This will guide and give directions and recommendations on how an organization can respond whenever a disaster strike.

REFERENCES

[1] Amin, M. E. (2005). *Social Science Research: Conception, Methodology and Analysis,* Makerere University Printery, Kampala.
[2] Bero L.A., Grilli R., Grimshaw J.M., Harvey E., Oxman A.D., Thomson M.A. Getting research findings into practice: closing the gap between research and practice: an overview of systematic reviews of interventions to promote the implementation of research findings. *BMJ.* 1998;317(7156):465–468.
[3] Bill, A. (2012). *5 Tips to Build an Effective Disaster Recovery*

Plan. Small Business Computing. Retrieved on 08.12.2016.

[4] Bolger, L. (2003). Scared or prepared? Disaster planning makes the difference. *Information Outlook*, 7(7), 25-31

[5] CDC. Strengthening Community Health Protection Through Technology and Training:The Health Alert Network. Report and Recommendations to the Appropriations Committee, United States Senate. April, 1998

[6] Chapman, J. (2005). Predicting technological disasters: Mission impossible? Disaster Prevention and Management: *An International Journal* 14, no. 3

[7] Comfort, L.K. (2005). Risk, security, and disaster management. *Annual Review of Political Science,* 8(1), 335-356

[8] Communication and Information Technology Commission .(2015). *Guidelines on Disaster*

[9] *Recovery Planning for the ICT Industry*. Kingdom of Saudi Arabia

[10] Creswell, J. W. (2014). *Qualitative inquiry and research design: Choosing among five*
a. *traditions*.Thousand Oaks, CA: SAGE.

[11] Dix, J. (2013). *Cloud computing causing rethinking of disaster recovery*. Retrieved on 08.12.2016 from http://www.networkworld.com/article/2168624/cloud-computing/cloud-computing-causing-rethinking-of-disaster-recovery.html. Network World

[12] Elaine,Pittman (2012).Emerging Technologies That Will Impact Emergency Management"

[13] Fraenkel, J.R., Wallen, N.E., and Hyun, H.H. (2012). *How to design and evaluate research in education (8th Ed.)*. Boston: McGraw Hill.

[14] Frankel, J. R, and Wallen, N.E. (2006). *How to design and evaluate research in education,* New York, McGraw- Hill.

[15] German Federal Ministry of Interior. (2005). *IT Emergency and Crisis Exercises in Critical Infrastructures.* Available online at https://. www.bmi.bund.de

[16] Haddow, G. D. and Bullock, J.A. (2006). *Introduction to Emergency Management*. (2nd ed.). Elsevier: Boston.

*[17] Hassan, Qusay (2011). "Demystifying Cloud Computing" (PDF). The Journal of Defense Software Engineering (CrossTalk) **2011** (Jan/Feb): 16–21. Retrieved 11 December 2014.*

[18] ISDR.(2002). *living with risk: a global review of disaster reduction initiatives*. Geneva: Switzerland.

[19] Jonathan Ellis(2014)Daily Nation newspaper, "*Failure of ICT Infrastructure in the Kenyan polls*" Sunday November 2, 2014 page 4, 1st Column

[20] Kothari, C. R. (2012). *Research Methodology: Methods and Techniques* (Second Revised Edition). Jaipur, Rajasthan, India: New Age International (P) Limited

[21] McEntire, D.A. (2004). Development, disasters and vulnerability: A discussion of divergent theories and the need for their integration. *Disaster Prevention and Management:* An International Journal 13, no. 3

[22] Myers Julie, Frieden Thomas R, Bherwani Kamal M, Henning Kelly J.(2008). Ethics in public health research: privacy and public health at risk: public health confidentiality in the digital age. *American Journal of Public Health*;98(5):793–801.

[23] Mnjama, N. and Wamukoya, J. (2007). E-government and records management: an assessment tool for e-records readiness in government", *The Electronic Library*, Vol. 25 Iss: 3, pp.274 – 284

[24] Patel, V. (2006). *Clinical Trials in Kenya. Amsterdam*. Stitching Onderzoek Multinationale Ondernemingen.

[25] Paton, D. and Johnston, D. (2001). Disasters and Communities: Vulnerability, resilience and preparedness, *Disaster Prevention and Management,* 10 (4): 270-277

[26] Quarantelli, E.L. (1998). *Where We Have Been and Where We Might Go. In:* Quarantelli E.L. (ed). What Is A Disaster? London: Rout ledge. Pp146-159

[27] Saunder, M., Lewis, P. and Thornhill, A.(2009). *Research Methods for Business Students* (5th ed.). Prentice Hall

[28] The East African Standard," Electronic voting was no panacea to election hitches" Wednesday, 31st July 2013

[29] Wang SJ, Middleton, B., Prosser et al.(2003). A cost-benefit analysis of electronic medical records in primary care. *American Journal of Medicine* 114:397– 403

[30] Williams, W.W. (2000). Library disaster planning and recovery handbook (book review). Library Journal, 125(11), 123.

[31] Wold, G. H. (1997). Disaster Recovery Planning Process. *Disaster Recovery Journal.* Adapted from Volume 1.