RECORDS AND INFORMATION DISASTER PREPAREDNESS IN SELECTED ORGANISATIONS IN UGANDA

Constant Okello-Obura
Department of Information Science, University of South Africa and
EASLIS, Makerere University
Email: obura@easlis.mak.ac.ug

Francis Ssekitto
EASLIS, Makerere University
Email: ssekitto@easlis.mak.ac.ug

Received: 2 March 2011
Revised: 25 June 2011
Accepted: 1 August 2011

Abstract

This study looked at the availability of rules and regulations governing access to and use of records; threats to records management; disaster response plan; extent to which organizations are committed in four major stages of disaster management in organizations in Uganda. In gathering the data, structured questionnaire was administered to 32 records and information professionals from both government and private sector who participated in performance improvement training in Electronic Records Management at Makerere University in August 2010. The findings show among others the areas of interest for short training for records managers; availability of rules and regulations governing access to records; percentage of the organizations' budget spent on disaster preparedness; threats to both paper-based and e-records; availability of policy on records disaster management; availability of migration plans from paper based to electronic records; rate at which records are lost through disasters. The study showed the level of records disaster planning preparedness of the organizations in Uganda and extent of commitment towards disaster management. It gives a picture of records managers' perception on aspects of records disaster management considered crucial for effective records management in organizations. The study concludes a worrying situation that requires immediate interventions that include among others: the need for

organizations to design records disaster management policy; the inclusion of disaster planning and management as a core training course for Information Science professionals; sensitization of organizations' policy makers on disaster planning and management; developing techniques for training, knowledge transfer and assessments for records disasters.

Keywords: Disaster Management, Records Disaster Plan, Records Management, Records-Threats, Uganda

Contextual background

Records consist of information recorded on paper, film, electronic and other media that are created or received by an organization in the day-to-day transaction of business activities. In today's world there are vast amounts of records that are being created digitally daily, and on paper and other recording formats and these are facts of the modern environment (Tale and Alefaio 2005). They provide the memory backbone and nerves for the efficient flow of business functions. For this to be achieved, disasters should be prevented. Przybyla and Huth (2004) observe that a records disaster is a sudden, unexpected event that significantly damages or destroys records or prevents access to the information they contain. A disaster does not have to be a widespread or catastrophic event (e.g. a tsunami, earthquake, volcano etc.) (ARMS 2006). It could be an insect infestation or could be something caused by human action such as a deliberately set fire or a bomb. The key attribute is that a disaster poses a threat to the physical safety and integrity of records (ARMS 2006). Organisations can significantly minimize the impact of a disaster in terms of property, business and even human costs if they recognize that disasters do happen and requires preparations to prevent their occurrence or minimize their impact. A disaster management plan can help avoid or manage events that can threaten, damage, or destroy records (Przybyla and Huth 2004). It is prudent to note that the process of planning, implementing and controlling the efficient, cost-effective flow and storage of records and information, from the point of creation to the point of consumption for the purpose of meeting the end beneficiary's or business requirements should be intertwined to proper disaster management

plans. Unfortunately, organizations especially in developing countries seem to pay little attention to records disasters planning.

Statement of the problem

The value of efficient records management in organisations can be equated to the value of well planned disaster management strategies in an organization. Iron Mountain (2004) observes that it is human nature to look at disasters/risks and assign a very low probability to their occurrence in businesses. It is only when disasters have occurred that managers of organizations seem to see the gravity of poor disaster preparedness. Most organizations seem not to have records disaster plans. In Uganda, we noticed this through interactions with two sets of participants who had come for in-service performance training course for records managers, archivists, registry staff and office administrators at East African School of Library and Information Science (EASLIS) in August 2010. During the group discussions, we realized that the issue of records disaster preparedness in most organizations was coming out strongly among the groups and this motivated us to design a strategy to study the records disaster preparedness in organizations in Uganda using the participants of the training course as the respondents.

1.3 Objectives of the study

The objectives of the study were to:

- Establish the availability of rules and regulations governing access and use to records in organizations in Uganda;
- Determine the threats to records management in organizations in Uganda;
- Find out whether organizations in Uganda have records disaster response plans;
- Establish the extent to which organizations in Uganda are committed in the four main stages of records disaster management; and

- Make recommendations aimed at improving on records disaster preparedness among organizations in Uganda.

Literature survey

All records and information materials regardless of form or medium created, received, maintained and used by an organization or an individual in pursuance of legal obligations or in the transaction of business must always be protected by organizations against disaster. The sections below review selected literature on the threats to records management; the need for disaster response plan and principles and practices of disaster preparedness planning for records and archives management in organizations.

Threats to records management

It should be noted that in spite of the different and in most cases irreplaceable functions of records to organizations of all sizes, there is a big danger that evidence of the past may be lost forever if these records are lost or destroyed. This can be attributed to exposure to records disasters. The security of records therefore should be well pronounced in well run organizations. Security of records refers to the measures instituted to safeguard records and information materials from being affected by human or non-human hazards or getting lost. All measures instituted for records security are aimed at ensuring that the records are not lost and kept for long due to their enduring value (Okello-Obura 2008). However, some of the threats may emanate from long-term neglect, and careless handling of records by even staff members of the organizations. Threats to records may include but are not limited to the following:

- *Disasters that stem from natural calamities*

Roper (1999) notes that these types of disasters originate from natural calamities and may be beyond the control of man. Such catastrophes include heavy earthquakes, flooding, tropical storms and lightning. This may be aggravated by the location of the records offices which may further expose the archival collections to heavy torrential rains, bush fires, lightning and heavy tectonic activity which may lead to earthquakes.

- *Another major cause of records deterioration is wear and tear*

This may be due to long term access and use or negligence of records by users. Abioye (2007) notes that most of the collections are transferred to the archives after they have been used in registries and gone through records centre. This cycle sees records used continuously and as such they lose their physical integrity. This is mostly true with paper based records which even lose some of the text on continuous use.

- *Environmental factors such as moisture owing to high levels of humidity and temperature are another notable cause of deterioration of records*

The Government of New South Wales (2002) notes that in principle the higher a temperature, the more quickly archival materials will deteriorate. This is because higher temperatures speed up the chemical processes that cause deterioration. Besides the temperatures are levels of humidity. It should be noted that in records offices, changes in relative humidity can have a negative effect on records. High relative humidity, particularly when coupled with high temperatures, accelerates the chemical deterioration of materials in the end quality/accuracy of the information in the document is affected.

- *Another critical source of deterioration to the archival collections is human activity*

Man/woman is considered the worst security threat to records in handling, storage, retrieval etc. (Okello-Obura 2008). This ranges from unintentional accidents, to intentional destruction and malice. It should be noted that deterioration relating to human activity account for most of the disasters that affect records around the world. Destructive human behaviour on the archival collections may include the following:

- Arsonists who deliberately start fires in records offices
- Careless handling of documents leading to wear and tear
- Malicious implant of viruses into electronic databases
- Plucking of pages from documents
- Poor retrieval and filing practices, causing materials to be torn
- Stealing of records material and illegal copying of documents
- Terrorism

- *Fungi, pests and moulds*

They weaken materials, causing ink to fade, material to fall apart and brown spots to appear. Such growths are caused by moisture in the

air. As ARMS (2006) notes insects/pests are a threat to records because they use them as a source of food (paper contains protein and starch) and their droppings cause damage that can deface or eliminate part of the text. Some parts of the world are more prone to insect infestation than others but records staff should regularly check all areas where records are stored to ensure there is no sign of insect infestation (ARMS 2006). If there is evidence of insect activity action should be taken to stop it, to decontaminate and to ensure it cannot start again.

- *Acidity in the ink and the paper on which the records are captured*

Acid is the worst enemy of records and archival materials. Acid is found in sulphur dioxide in polluted air, in lignin in wood pulp, in the products and chemicals used to make paper (Okello-Obura 2008). Acid can weaken and damage paper.

- *Pollution especially by cars and the activity from industrial locations that are in proximity with records offices*

It should be noted that an institution can significantly reduce the impact of the above threats if it recognizes that disasters do happen and that there is need to proactively work to anticipate and prevent them.

Electronic records are also not spared by threats. Some of the common threats to e-records include:

- *Computer Viruses, Worms and Trojan Horses*

A virus is a potentially damaging computer program that affects or infects a computer negatively by altering the way a computer works. A worm on the other hand is a program that copies itself repeatedly, for example in memory or on a network and possibly shutting down the computer. While a Trojan horse is a program that hides within or looks like a legitimate program. Unlike a virus or worm, a Trojan does not replicate itself to other computers. All these are threats to all electronic records without protective measures. The symptoms of viruses, worms and Trojan horses include:

- Screen displays unusual messages or image
- Music or unusual sound plays randomly
- Available memory is less than expected
- Existing programs and files disappear
- Files become corrupted
- Programs or files do not work properly

- Unknown programs or files mysteriously appear etc (Senn 2004).

- *Spyware* - A spyware is a program placed on a computer without the user's knowledge that secretly collects information about a user. Spyware can enter the computer through a virus or as a result of installing a new program. The spyware program communicates information it collects to some outside source while one is online. Spyware has evolved, becoming yet another category in a growing list of malware. Some spyware can install rootkits, keyloggers, redirectors, and software intended to exploit application vulnerabilities. Several of these spyware applications use operating system exploits to install affiliate and other unwanted, unrequested software programs (Websense 2007). Others attempt to gain network access in order to steal CPU or network cycles, to install more applications on the system, or enable the theft of proprietary information, including proprietary company data such as client databases, customer information, and so on (Websense 2007).
- *Cyberterrorism* - It is where someone uses the Internet or network to destroy or damage computers for political reasons. This can happen with government organizations and is a threat to the security of records management.

Generally, there are many threats to both paper based and electronic records in organizations that if not prevented can lead to the collapse of an organization. Organisations need to have in place strategic plans to avert crisis or disasters or security of records from being compromised.

The need for disaster response plans for records

Many institutions around the world and Uganda in particular conduct their normal business as though they will never experience a disaster. Przybyla and Huth (2004) note that many organizations never develop strategies for preventing or responding to disasters. Even those that have formal disaster management plans largely neglect aspects of protecting on their most valuable assets; their records (Gerber 2007). A review made by Hlabaangani and Mnjama (2008) indicates that in Africa, the incidence of disasters is well captured by Alegbeleye (1993) who states that a number of disasters have struck information centres, and a lot of damage has been done to records,

books and artifacts. Alegbeleye (1993) observes that in 1988, records were destroyed when a record centre was burnt down by students in Sierra Leone. In another incident, the Nigerian Institute of Policy and Strategic Studies Library experienced electrical failure resulting in a fire which destroyed many books, artifacts, and other monuments in 1987. In Kenya, the then Colonial Secretary Office's containing early colonial records was gutted down by fire in 1939, resulting in considerable loss of valuable records (Hlabaangani and Mnjama 2008). A survey of disaster management in academic libraries in Ghana carried out by Akussah and Fosu (2001) revealed that there were varying levels of disaster preparedness by libraries and archives. Their study further revealed that libraries were characterised by lack of disaster plans, inadequate human and material resources, and lack of conservation workshops to restore damaged information materials (Akussah and Fosu 2001).

The Department of Disaster Management and Refugees, Office of the Prime Minister, Uganda (2004) notes that disasters are rampant in Uganda. The earliest recorded disaster was an earthquake in 1897. These disasters have caused a great deal of suffering and loss of property and productive capacity for the peoples of Uganda. In so doing, disasters have contributed to the retardation of social development (The Department of Disaster Management and Refugees, Office of the Prime Minister, Uganda, 2004). This kind of scenario motivates us to ask whether there is national policy, strategy and legislation addressing disaster risk reduction in Uganda. The answer is YES**.** Uganda has in place a National Disaster Preparedness Policy and Institutional Framework approved by Cabinet in 1999 and revised in 2003. In addition Uganda has in place a National Policy on Internal Displacement of Persons. Unfortunately, there is no specific and known policy and legal frameworks to handle records and information management disasters in Uganda among government organizations. The involvement of institutions on disaster management outside Government of Uganda is still very low. Disaster risk reduction in Uganda is a new phenomenon (The Department of Disaster Management and Refugees, Office of the Prime Minister, Uganda, 2004). These clearly indicate that there is need for countering disaster.

The Government of South Australia (2007) notes that counter disaster management is the term given to strategies for the prevention, preparedness and response to disasters, and the recovery of operations following disasters. Counter disaster management for records should take place in the framework of a government agency's business continuity plan. Within that framework there are 4 stages according to the Government of South Australia (2007):

- assessment of risks affecting records and recordkeeping systems, and the subsequent activities to reduce the probability of a disaster and reducing the probability of loss should a disaster occur;

- planning activities to establish a counter disaster plan to assist the government agency to respond to an emergency event ;

- the activities to identify and protect vital records of the agency; and

- response and recovery from a disaster: the activities involved in implementing the plan and initiating resources to protect or secure the organization from loss, and restoring records and operations, so that normal business operations can resume.

The need for disaster response plans for records in any given organization/government or otherwise can be identified from the leverage that such plans give to organizations that invest efforts to their deliberate proliferation. Estrella-Luna and Pearson (2002) argue that the value of planning in disaster management can never be underestimated by any serious business organisation. They note that the potential for disaster can be reduced by identifying and correcting hazardous conditions and by encouraging staff alertness in detecting and reporting problems. As Ngulube and Magazi (2006) note, disasters cannot be entirely prevented, but there is need to be prepared for them so that their negative effects may be minimized in organisations. Disasters do not discriminate where to strike and therefore adequate plans should be made before hand. Preparing for disasters requires an ongoing commitment to reduce potential disasters and develop a plan of action for response to disasters.

Showing salvage priorities; floor plans and maps; simple technical information on the handling of damaged material, directed towards establishing priorities for early action are considered crucial in disaster management plan construction.

The need for a records management disaster plan helps in devising early detection of any threats to records, mitigating them before they strike and also to limit damage when disaster strikes. The records management disaster plan will also provide a systematic procedure for business continuity when disaster strikes. However, it was not well known as to whether organizations in Uganda have records and information disaster management plans. This situation was established in this study.

Principles and practices of disaster preparedness planning for records and archives in organizations

Management of risks and disasters to records in any organisation requires an exercise of strong judgment (Alegbeleye, 1993). The management of disasters to records is guided by five main principles and these principles are applicable to all forms of records, from paper based records to electronic records and micro-films. These principles according to Rhys-Lewis (2000) include the following;

- Risk assessment - assessing the dangers to the building and the collections
- Prevention - implementing measures to remove or reduce danger
- Preparedness - the detail of the plan itself
- Response - the planned procedures to follow
- Recovery and business continuity- restoring the site and material to a stable and usable condition (Rhys-Lewis 2000).

The assessment of risk involves the identification of risks to which an enterprise is liable. This identifies both the external and internal environmental threats. Prevention includes the level of routine building maintenance carried out and the degree of provision of fire alarm and fire suppression systems. Preparedness does require detailed floor plans and the establishment of priority lists of the stored material (Rhys-Lewis, 2000). This consist of a range of management activities, such as regular reviews of incidents (however minor), the identification of salvage areas, the training of staff and the

establishment of teams to carry out the specific salvage activities. There is also a need for a significant commitment to the research of local facilities, including freezer and transportation services. Careful consideration will be required to identify adequate budgets for the purchase of emergency supplies. Educating the public and others involved in the planning process on keys issues regarding disaster preparedness is always considered crucial (Rhys-Lewis, 2000).

Quarantelli (1984) and Burling and Hyle (1997) note that organizations should promote the following general principles of disaster preparedness planning if security of records and good maintenance is to be provided:

- convening meetings for the purpose of sharing information;
- holding disaster drills, rehearsals and simulations;
- developing techniques for training, knowledge transfer and assessments;
- formulating memoranda of understanding and mutual aid agreements;
- educating the public and others involved in the planning process;
- obtaining, positioning and maintaining relevant material resources;
- undertaking public educational activities
- establishing informal linkages between involved groups in records management processes;
- thinking and communicating information about future dangers and hazards; and
- drawing up organizational disaster plans and integrating them with overall community- mass-emergency plans; and continually updating obsolete materials/strategies.

An analysis of the principles above shows that it is a reflection of three general groups of issues or concerns. These are education, information dissemination and practice. By induction any principles and practices behind disaster preparedness planning should dovetail education, information dissemination and practice (Burling and Hyle 1997).

Finally, recovery requires management to set priorities, liaise with the media, clean and rehabilitate the site and ultimately review the plan. Alegbeleye (1993) however notes that in the management of records today where electronic media is, the disaster management plan

should involve or make provisions for records backup so that organizations have fall back positions when disaster strikes.

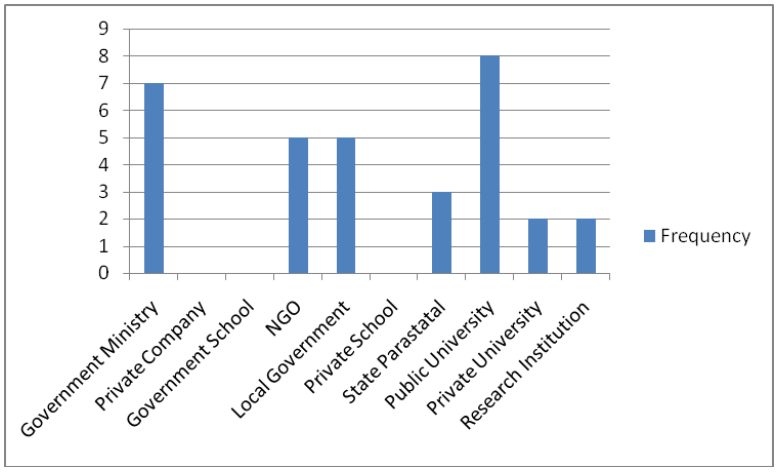
Methodology

The study used a quantitative approach in which structured questions were used for data collection. The questionnaire was structured into 4 main parts, namely, background information of the respondent; availability of rules and regulations governing access and use to records; threats to records management and disaster response plan. The questionnaire was administered during a short training course on Electronic Records Management that was held in August 2010 at EASLIS, Makerere University. The questionnaire was given to two lecturers who teach records and archives management at EASLIS to critique before it was administered. The questions were thereafter adjusted based on the criticism. Of the total of 37 participants for the short course, 32 responded to the study. After data collection, the responses were cross checked for clarity and legibility by the Lead researcher before entering the data into the computer using the Excel program.

Background information of the respondents

Of the expected 37 participants, 32 respondents participated giving a response rate of 87% and of these, there were 34.4% male and 65.6% female. The organizations where the respondents are employed are classified as indicated in Figure 1.

Figure 1: Classification of the organizations in which respondents work



An analysis of Figure 1 indicates that private company, government schools and private schools had none who participated in the inservice training on electronic records management (ERM). On contrary, Government Ministry, Public University and Local Government had good participation in comparision. According to Uganda, Ministry of Public Service (2005:8), records management systems in Uganda are not fully developed. Records are not captured and stored in a systematic and easy to retrieve manner due to among others lack of well-trained human resources. This good attendance could be a realisation by the Government of Uganda of the values attached to records management, the need to improve on records management and the adoption of e-govervance as stratregic means to improve on government service delivery. Without adequate skills in ERM, there is no way e-governace can be promoted. Records staff need to have skills in ERM to promote e-governmence.

When respondents were asked to state as to whether they had any qualifications in records management, the responses were as indicated in Figure 2.

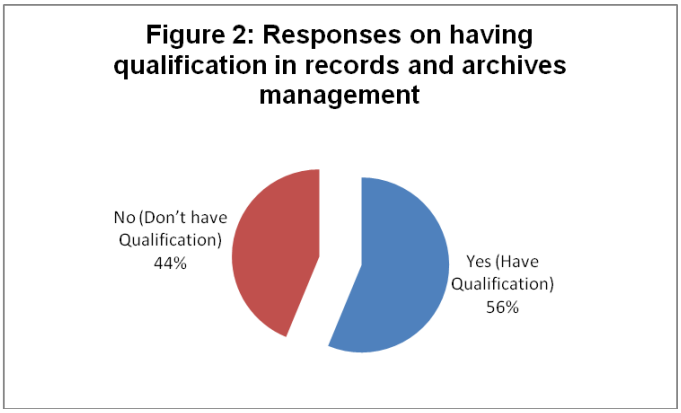


Figure 2 indicates that quite a number of organisations in Uganda did not have qualified personnel in records and archives management although they are managing records in their organisations. This could be attributed partly to the fact that Library and Information Science Education institutions for a very long time have concentrated on training librarians. It was until 1999 when EASLIS, Makerere University started a Diploma in Records and Archives management and in 2009 started a Bachelor of Records and Archives Management. It should be noted that the quality of human resources is critial in planning and developing strategies for good records

management. When you observe Figure 3, you notice that the majority of the organisations have ever lost vital records. Though there could have been other factors that contributed to this we can not rule out the incompetencies of the staff entrusted with the responsibility of records management. Qualified staff are in a better position to articulate strategies and policy issues that impact positively on records and archives management.

Regarding the short course training the respondents would prefer to go for, the results are as given in Table 1.

Table 1: Preferences of Respondents on the short courses they would go for when given opportunity

Short Courses	Responses
Database management	25%
Internet technologies	9.4%
Disaster management for records	19%
Archival preservation	9.4%
Digital preservation	9.4%
Office management and ethics	9.4%
Legal issues in records management	16%
Financial records management	3.1%
Local government records management	-

An observation of Table 1, indicates that there are different areas of competencies required by records managers in the organisations in Uganda. Singled out is the Database management (25%), Disaster management of records (19%) and Legal issues in Records management (16%). An interesting finding was on the lack of interest in short course in local government records management although there were participants from Local Government. This is an indication that Local Government records managers do not see anything new in particular to learn about local government records except and probably cross cutting courses like Database management and Records Disaster management. The interest in disaster management is encouraging.

Given that the organisations in Uganda have ever expressed concern on the lost of vital records due to disaster occurances (see Figure 4), this implies that viable strategic interventions that are proposed by

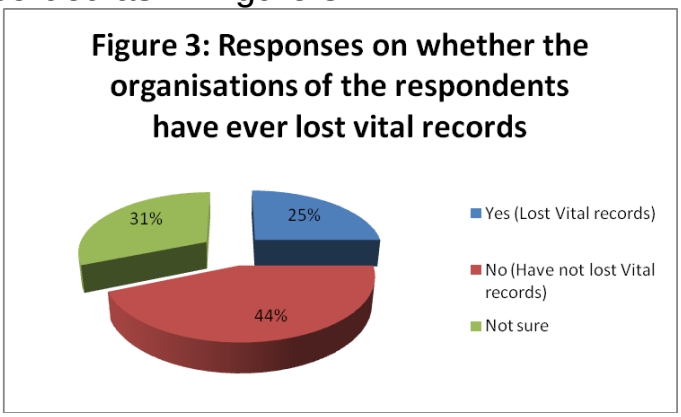
records management staff towards records disaster management in organisations could be ably suported by the organisation management. Although management showed concern when vital records were lost, this in our view should be reflected in the budget committement to records disaster management. An observation of Figure 6 shows that the level of budget committement of the majority of the orgainisations towards records disaster management is negligible. This probably confirms the observation by Tale and Alefaio (2005) that,

> the field of records management has traditionally been viewed with little if any significance. This continues today. Records management in developing countries is yet to attain the level of attention and support that it receives in countries of the developed world.

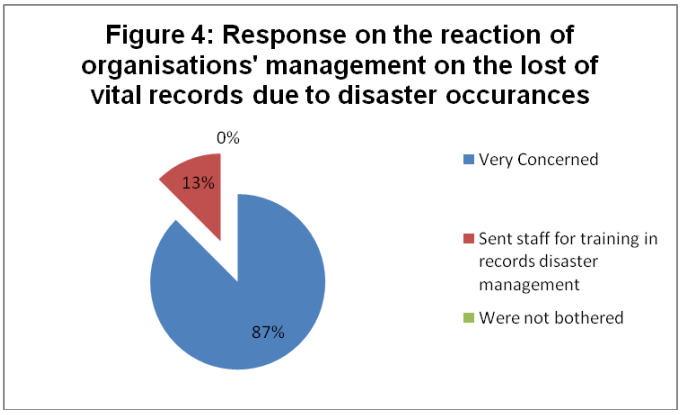
Management of organisations need to change this attitude. Commitment to records disaster should be reflected in budget allocation to records mangement matters.

Availability of rules and regulations governing access and use of records

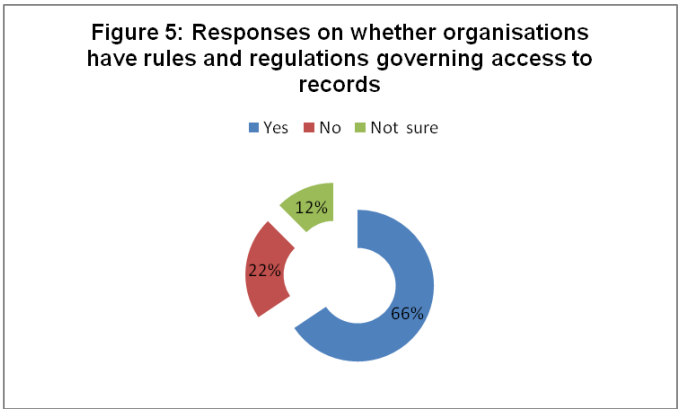
Loss of vital records due to disaster occurrences, were established and results recorded as in Figure 3.



When those who said yes in Figure 3 were asked to give the reaction of management towards records lost, the responses were as in Figure 4.



Regarding the organisations that have rules and regulations governing access to regards, the responses were as in Figure 5.

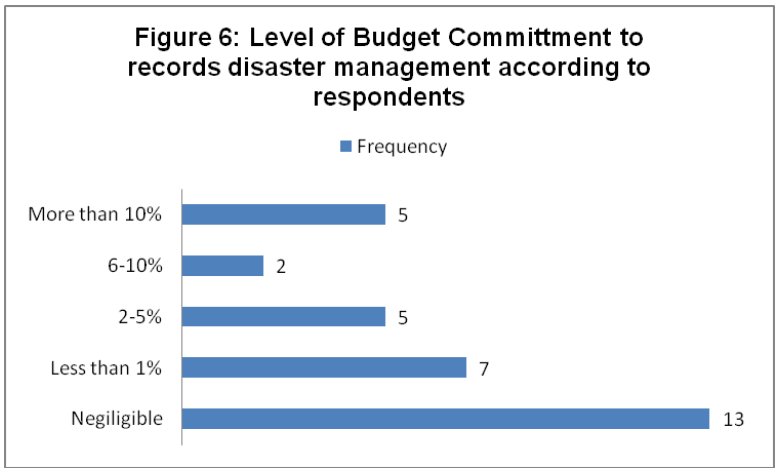


When those who indicated that their organisations have rules and regulations governing access to records were asked to state how the rules and regulations were publicised in the organisations, the responses were as indicated in Table 2.

Table 2: Responses on the methods of publicizing rules and regulations governing access to records

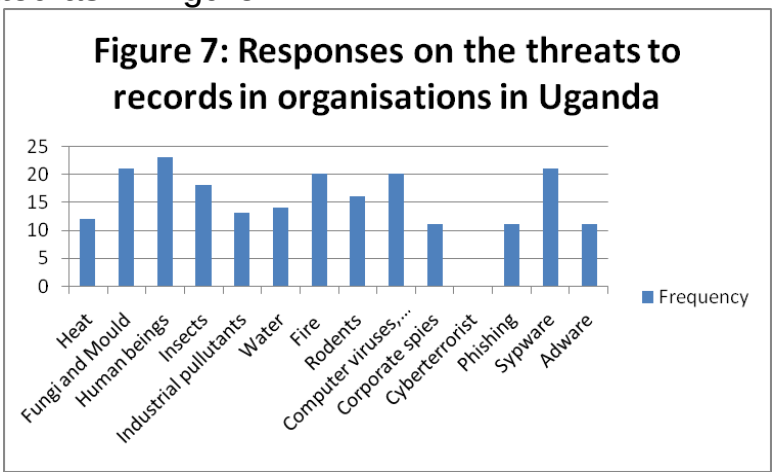
Methods of publicizing rules and regulations	Response
Through notice boards	24%
Through the organization's websites	19%
Through regular memos	24%
Through word of mouth	19%
Not publicized to any body	14%

The study also found it important to establish through the participants the percentage of the organisations' budget that is committed to records disaster management and results were as given in Figure 6.



Threats to records management

The treats to records management in the organisations in Uganda were indicated as in Figure 7.



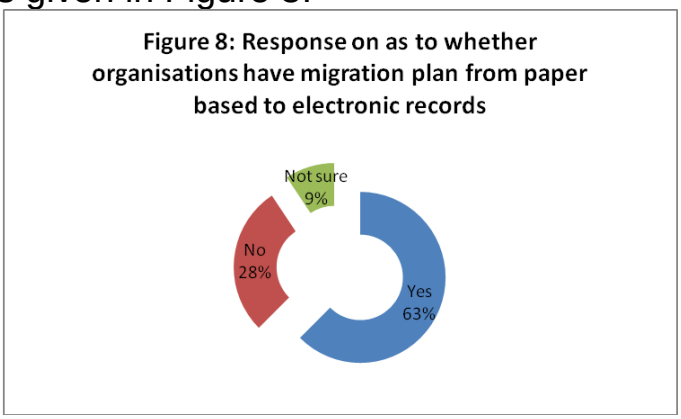
When a list of disasters were given to the respondents and asked to indicate the extent to which they were threats to records in their organisations, the results were as given in Table 3.

Table 3: Extent to which different threats are on records in different organizations in Uganda

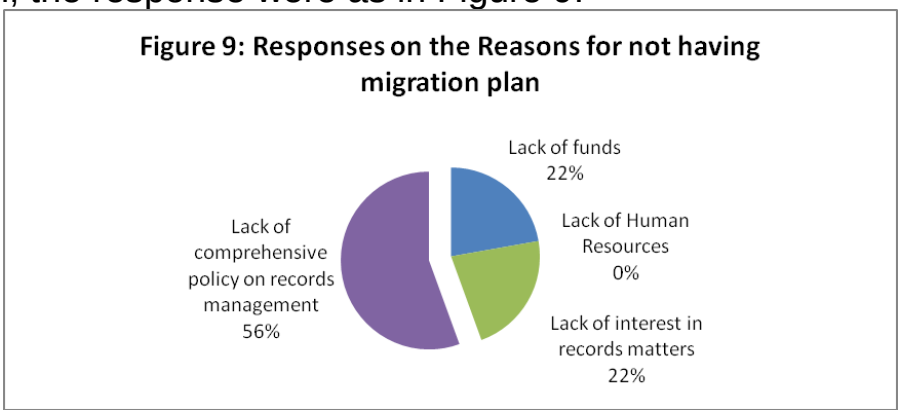
Treats	Very Dangerous	Dangerous	Not Dangerous
Natural events such as earthquakes, bushfire, flood, vermin etc	25%	31%	44%
Structural or building failure e. g. Poor wiring, leaks of roof	22%	31%	47%
Poor storage conditions (weak boxes, acidic shelves and boxes)	31%	36%	31%

Treats	Very Dangerous	Dangerous	Not Dangerous
Industrial accidents such as nuclear or chemical spills	25%	28%	44%
Criminal behaviour such as theft, arson, vandalism, riots, terrorism and war	38%	41%	19%
Technological disasters such as viruses and computer equipment failures	31%	53%	16%
Accident lost through human errors	50%	34%	16%

When the respondents were asked as to whether their organizations had any migration plan from paper based to electronic records, the results were as given in Figure 8.

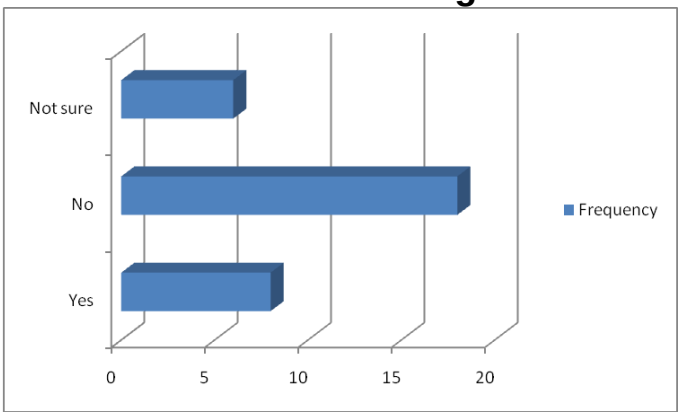


When those who said No were asked of what should have been the problem, the response were as in Figure 9.

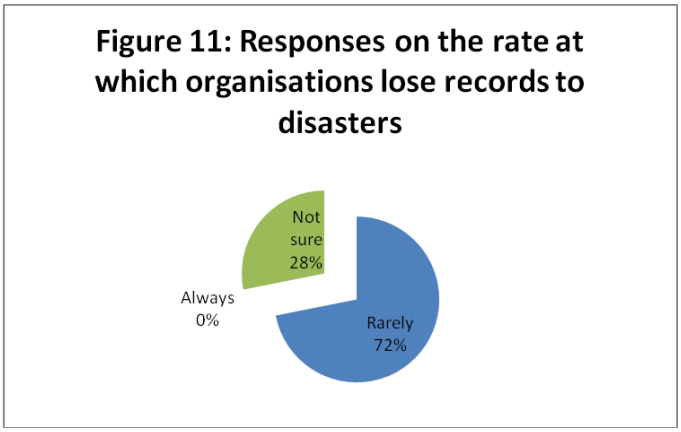


Regarding policy on records and information disaster management, the response were as given in Figure 10.

Figure 10:Response on whether organisations have policy on records disaster and information management



Respondents were asked on how often their organisations lose records and information to disasters and the responses were as in Figure 11.



An analysis from Figure 5 indicates that, 66% accepted that their organisations have rules and regulations and Table 2 shows that these rules and regulations are publicised using different methods but regretably 14% of the organisations do not publicise these rules and regulations to anybody. For any organisation to function effectively, there must be systems that are respected and within these systems there are rules and regulations that are known and must be adhered to. However for 22% (see Figure 5) of the organisations not to have rules and regulations is an issue of concern. Perfection and efficiency are compromised without rules and regulations governing the operation of records and information systems in an organisation. For instance, an observation of Figure 7 indicates that the records in organisations are heavily threatened ranging from human beings, fungi and mould, fire, computer virues to spyware. This confirms what

Government of South Australia (2007) observed that thousands of records facilities worldwide have suffered damage in disasters. The only threat not experienced by organisations in Uganda as noted in Table 7 in relation to records management is the cyberterrorism.

A further probe into the extent to which different threats are on records and information in different organisations shows that the most dangerous threat is accident lost through human errors. This coupled with criminal behaviour such as theft, arson, espionage, vandalism, riots, bombing, demonstrations, terrorism and war pose a serious threat to records in organisations. Technological disasters and poor storage conditions are also significant threats to records in organizations in Uganda. Organisations need to make attempts to breach records security threats arising from employees, hackers, terrorists and other technological risks (Senn 2004).

These can be ably handled with an approved and supported organization policy on records disaster preparedness. To even make matters worse, most of the organizations do not have policy on records disaster management (see Figure 10). This confirms what Ngulube (2005) demonstrated in his studies, that disaster preparedness and security of records and archives did not form a significant part of the preservation activities of archival institutions in most organisations. He further notes that too many archives institution in ESARBICA region have neither a disaster preparedness policy nor security plans in place (Ngulube 2005). There is urgent need for organizations without a policy on records disaster management to develop one if threats and other record disaster occurrences are to be minimized. Tale and Alefaio (2005) ably note that the absence of policies to provide guidance to creators and users of records poses risks that cannot be ignored by any organization interested in posterity.

Disaster response plan

When the respondents were asked on what they would consider in the records disater response plan, the responses were as in Table 4. From Table 4, regarding what respondents would consider to include in the disaster response plan, the majority (72%) indicated salvage priorities followed by proceedures for identification and declaration of

a disaster situation and listing of back-up resources, including expertise and local emergency personnel. The overall views of the respondents show that they were aware of the important aspects to consider in a disaster response plan. As Przybyla and Huth (2004) note, the goal of planning a disaster response is to ensure the safety of the organisation's records under stressful circumstannces and to allow the swift resumption of normal business operations. Although some organisations do not have records disaster management policy as noted in Figure 9 which is unfortunate, most organisations have some general principles being practiced regarding disaster preparedness planning. This situation makes one to be forced to think that without a policy, the general principles of disaster prepareadness planning indicated in Table 5 are being practiced hapazardly.

Table 4: Responses on what respondents would consider to include in the disaster response plan

Items	**Response (%)**
Salvage priorities- List of vital records, their location and control documentation	72
Procedures for the identification and declaration of a disaster situation and initiation of the disaster response chain of command	63
List of the equipment and material available for use in disaster salvage and recovery	44
Floor plan and areas maps – Supplement narrative information with floor plans that provide salvage priorities	50
The function, composition and chain of command of the salvage and recovery team and their contact details	44
Provision for the training and current awareness of the salvage and recovery team	59
List of sources of back up resources, including expertise, material, equipment, local emergency personnel etc	63
Procedure for updating and testing the plan	50
Simple technical information on the handling of damaged material, directed towards establishing priorities for early action.	47

When the respondents were asked to state the general principles of the disaster preparedness planning practiced in their organisations, the response were as given in Table 5.

Table 5: Responses on the general principles of disaster preparedness planning practices in organizations

Principles	Response (%)
Convening meetings for the purpose of sharing information;	47
Holding disaster drills, rehearsals and simulations	38
Developing techniques for training, knowledge transfer and assessments for records disasters	44
Formulating memoranda of understanding and mutual aid agreements aimed at protecting records from disaster occurrences;	38
Educating the public and others involved in the planning process on keys issues regarding disaster preparedness	38
Obtaining, positioning and maintaining relevant material for disaster control e.g. fire extinguisher	56
Undertaking public educational activities on records disaster management for hazards control	38
Establishing informal linkages between involved groups	44
Thinking and communicating information about future dangers and hazards	44
Installation of fire, water and movement alarms	44
Drawing up organizational disaster plans and integrating them with overall community-mass-emergency plans	38
Placing priority on vital records and critical data recovery	44
Establishment of an information security program to protect information	50
Establishment of prevention, response and recovery contracts so that vendors can be on hand in emergency	38

It was also found important to establish the extent to which organisations were committed to the four main stages of disater management and the results were as given in Table 6:

Table 6: Responses on the extent to which organizations are committed to the four main disaster management phases

Stages of disaster management	Very committed	Committed	Somehow committed	Not committed
Prevention (Disaster mitigation)	31%	28%	25%	13%
Preparation- The goal is to achieve a satisfactory level of readiness to respond to any emergency situation	22%	34%	28%	16%
Response to disaster	25%	28%	22%	25%
Recovery after disaster	19%	31%	19%	31%

The four main areas of disaster management include: prevention, preparation, response to disaster and recovery to disaster (Government of South Australia 2007). When you observe the results in Table 6 carefully, you notice that the organisations are committed to all the four stages of disaster management. The only question that remains lingering in the mind is, how are they committed without comprehensive policy guidelines on records management as indicated in Figure 9? We are forced to say that although the organisations are committed to the four stages of disaster management, they are handling disaster management in an haparzard manner and that is itself a **disaster**!

Conclusion and recommendations

Records are always potentially at risk of disaster. Due to the importance of records, their loss in a disaster can be crippling for the responsible government or business agency. Every organization needs to seriously plan and execute strategic measures to ensure that the memory of organisation - (records) is kept free from sudden destructive occurrences.

Despite the appalling situation in some organizations in Uganda regarding records disaster management, and in many developing countries, there are some bright spots that need to be tapped. There are developments such as e-governance programmes, public sector reforms, the pressure from civil society for good governance and other activities happening in Uganda which in our view offers opportunities to make a positive impact in many organizations in Uganda and the society as a whole. These opportunities should encourage records managers, LIS educators and records and archives policy makers to reposition themselves, develop arguments and take positions, strategize, and involve themselves in trying to find solutions to common problems that are related to records disaster management. It is evident from this study that there are general concerns within organizations about records disaster management but the effective applications of the best practices to avoid disasters are being hampered by lack of budget support and comprehensive policy guidelines for managing records disasters. This study thus recommends as follow:

- Organizations in Uganda should as a matter of urgency develop comprehensive policy guidelines/frameworks for the management of records disasters. This should include both paper based and electronic records. The disaster plan must include a series of steps for staff to follow, beginning with the initial discovery that something is wrong. Issues like records migration plans should be clearly stipulated in the plan/policy.
- The Government of Uganda and other organizations should treat records as a crucial component for efficient and effective management by making significant budget commitment to activities such as disaster management.
- EASLIS, Makerere University including other LIS training institutions in Uganda in consultation with different organizations in Uganda should design a curriculum in Records Disaster Management and staff from different organisations including policy makers is sensitized on records disaster management.
- The organizations in Uganda should be encouraged to have disaster response plan that include among others: List of vital records, their location and control documentation, Procedures for the identification and declaration of a disaster situation and

initiation of the disaster response chain of command, List of the equipment and material available for use in disaster salvage and recovery, Floor plans and area maps, The function, composition and chain of command of the salvage and recovery team and their contact details, Provision for the training and current awareness of the salvage and recovery team, List of sources of back up resources, including expertise, material, equipment, local emergency personnel etc, Procedure for updating and testing the plan and simple technical information on the handling of damaged material, directed towards establishing priorities for early action. This Plan should be easily accessed by all staff in the organization.

- EASLIS and other LIS training institutions should integrate records disaster management as a core course in their training programmes.
- The general principles of disaster preparedness planning practiced in organizations in Uganda as elaborated in Table 5 should be strengthened by putting in place a policy framework with a clear supervisory roles for records disaster management team. A well organized collaborative strategy should be designed between organizations with other agencies such as fire departments that deal with disaster management.
- The Government of Uganda just like having a national framework for National disasters under the Prime Minister's Office should provide a national framework for disaster management for records and archival materials. It is expected that if the government sets a way forward, the private sector would follow.

References

Abioye, A. 2007. Fifty years of archives administration in Nigeria: lessons for the future. *Records Management Journal* 17(1): 52-62.

Akussah, H. and Fosu, V. 2001. Disaster management in academic libraries in Ghana. *African Journal of Library, Archives and Information Science* 11(1): 1.

Alegbeleye, B. 1993. *Disaster Control Planning for libraries, archives and electronic data processing centers in Africa*. Ibadan: Options Book and Information Services.

ARMS. 2006. Emergency preparedness for a mission storage, United Nations. [Online]. Available WWW: http://archives.un.org/ (Accessed 25 March 2011).

Burling, W. K. and Hyle, A. E. 1997. Disaster preparedness planning: policy and leadership issues. *Disaster Prevention and Management* 6(4): 234-244.

Estrella-Luna, N. and Pearson, P. 2002. *The State University of West Georgia records disaster management plan*. Georgia: State University of West Georgia.

Hlabaangani, K. and Mnjama, N. 2008. Disaster preparedness in information centres in Gaborone, Botswana. *African Journal of Library, Archives and Information Science* 18(1): 3-10

Iron Mountain. 2004. The business case for enterprise disaster recovery planning: calculating the cost of downtime, White paper, contingency planning and Management, January 2001.

Gerber, B. J. 2007. Disaster management in the United States: examining key political and policy challenges. *Policy Studies Journal* 35(2): 227-238.

Government of New South Wales. 2002. *Guidelines on counter disaster strategies for records and recordkeeping systems*. Sydney: Government of New South Wales.

Government of South Australia. 2007. Records management disaster planning guideline. Version 1.1. [Online]. Available WWW: http://www.archives.sa.gov.au/files/management_guidelines_ARM_disasterplanning.pdf (Accessed 25 March 2011).

Ngulube, P. 2005. Disaster and security management in public archival institutions of the East and Southern Africa Regional Branch of the International Council on Archives (ESARBICA) member states. *African Journal of Library, Archives and Information Science* 15(1): 15-23.

Ngulube, P. and Magazi, L. 2006. A stitch in time saves nine: emergency preparedness in public libraries of KwaZulu-Natal, South Africa. *Innovation: appropriate librarianship and information work in Southern Africa* 32: 110-124.

Okello-Obura, C. 2008. Records security: a paper presented in the workshop on Records and Information Management at East African School of Library and Information Science Makerere University, 28 July - 1 August 2008.

Przybyla, A. M., and Huth, G. 2004. *Preparing for the worst: managing records disasters*. New York: The University of the State of New York.

Quarantelli, E. L. 1984, Organizational behavior in disasters and implications for disaster planning. *Monographs of the National Emergency Training Center* 1(2): 1-31.

Rhys-Lewis, J. 2000. *Conservation and preservation activities in archives and libraries in developing countries: an advisory guideline on policy and planning*. London: Association of Commonwealth Archivists and Records Managers. [Online]. Available WWW: http://www.acarm.org/documents/Guidelines%20on%20Preservation.pdf, (Accessed 2 March 2011).

Roper, M. (ed.) 1999. *Preserving records*. London: International Records Management Trust.

Senn, J. A. 2004. *Information technology: principles, practices, opportunities.* 3rd ed. New Jersey: Pearson Education.

Tale, S. and Alefaio, O. 2005. Records management in developing countries: challenges and threats – towards a realistic plan. *ACARM Newsletter* 37(Winter). [Online]. Available WWW: http://www.acarm.org/documents/issue37/37 (Accessed 25 March 2011).

The Department of Disaster Management and Refugees, Office of the Prime Minister, Uganda. 2004. Uganda National report and information on Disaster risk reduction efforts for the world conference on disaster reduction (Kobe-Hyogo, Japan, 18-22 January 2005). [Online]. Available WWW: http://www.unisdr.org/eng/country-inform/reports/Uganda-report.pdf (Accessed 18 May 2011).

Uganda, Ministry of Public Service. 2006. *Public Service Reform Programme Strategic Framework (2005/6-2009/10).* Entebbe: UPPC.

Websense. 2007. Protecting organizations from spyware. [Online]. Available WWW: https://www.websense.it/assets/white-papers/Protecting-Organizations-from-Spyware.pdf (Accessed 25 March 2011).