International Journal of Risk and Contingency Management
Volume 5 • Issue 1 • January-March 2016

Disaster Management in Digital Libraries:
Issues and Strategies in Developing Countries

Goodluck Ifijeh, Covenant University, Ota, Nigeria
Jerome Idiegbeyan-ose, Covenant University, Ota, Nigeria
Chidi Segun-Adeniran, Covenant University, Ota, Nigeria
Julie Ilogho, Covenant University, Ota, Nigeria

ABSTRACT

The role of digital libraries in information generation,organization, dissemination and storage cannot be overemphasized. This article articulates the importance of digital libraries and the need to preserve them from disasters. It highlights the causes and effects of disasters in digital libraries. Prevention and management of disasters were also discussed. Issues and challenges around information and communication technology (ICT), that has direct bearings on digital libraries and disaster management in developing countries were raised. In addition, recommendations were made on how to improve on disaster prevention and control.

KEYWORDS:

Computer Security, Data, Developing Countries, Digital Divide, Digital Library, Disaster, Disaster Management, ICT Policy

INTRODUCTION

Since the turn of the 21st century, libraries have been drifting from the utilization of manual methods of operations to automated methods. The resources made available in the libraries are also being repackaged in virtual or electronic format. It is this drift that has brought about the concept of digital libraries (Ottong and Ottong, 2013,p.99).

Digital libraries carry out specialized library services and functions to users through automated methods or machine readable formats. Nwalo (2011, p.32) described digital libraries as any of the following:

- Collection of electronic journals and books
- Repository of multimedia files
- Digital archives of information created from local knowledge
- Electronic version of libraries.

Despite the advantages derived in the use of automated methods in carrying out library and information services, the occurrence of disasters in these digital libraries can not be ruled out and have become matters of great concern globally. This is because disasters are often inevitable. Ottong and Ottong (2013) defined a "disaster as any incident which threatens human safety and /or damages, or threaten to damage, a library's buildings, collections (or items therein), equipment and systems"

DOI: 10.4018/IJRCM.2016010101

(p.100). Disasters could be linked to physical, environmental and technological factors such as explosion, loss of power, internet failure, flood, etc.

The advent of digital libraries has increased the occurrence of disasters caused by technical and technological factors. These could include hampering of library operations and loss of vital data caused by such technical factors as hacking into library online records, virus damage to records, systems crash and breach in computer security systems, etc. A critical examination of the concept of disasters in digital libraries, with a view to reducing their occurence to the barest minimum, would require an indepth analysis of current management, control practices, and needed improvements.

This article outlines the causes and effects of disasters in digital libraries and makes recommendations for developing countries.

CAUSES OF DISASTERS IN DIGITAL LIBRARIES

Disaster in digital libraries implies any incident that may cause threat or damage to digital documents in the holdings of a library. Disaster management activities for digital information resources arise from real and imagined threats (Anderson, 2005 and Cervone, 2006). The causes of disasters in digital libraries can be accrued to various factors. According to Altman et al. (2009, p.171), these can be broadly categorized into four groups:

- Physical threats
- Technological threats
- Human threats
- Institutional threats

Physical Threats

These are causes of disasters in digital libraries that come about as a result of some natural effects which could be controllable and in some instances uncontrollable; age, storage facilities, fire and some natural disasters.

Similarly, physical threats in a digital library could also be as a result of failure of some of the information technology media and infrastructure used in the digital libraries. Except in cases where the electronic resources or bibliographic details of resources available in the library are stored in the cloud; the resultant loss of data and information resources could pose far reaching educational and economic consequencies to any community.

Technological Threats

Technological threats could as be as a result of hacking, utilization of outdated gadgets, virus attacks, data loss due to inadequate back up etc.

- **Hacking:** This can be simply explained as a process of intruding or gaining improper, unauthorized and illegal access into a computer system. It is usually dangerous to the system; it is simply defined as theft because the proper protocol for accessing information is not followed. Dunning (2014) defined computer hacking as "a means or process of gaining unauthorized access to computer and network resources often, but not always, with malicious intent" (para.1).It is important to note here that not all hacking attempts are with the intention or motive of causing harm; but it does not overrules the fact that it is risky to the computer systems and the information stored therein especially in a digital library where virtually all the records and information resources are digitized and stored in computer systems. Dunnings (2014) also reiterated that hackers break into computer systems by exploiting security vulnerabilities, such as poor configuration of Web servers, disabled security controls or poorly chosen or default passwords, he observed that "Hackers

may modify existing computer resources and settings without consent and, in so doing, cause damage or disruption to computer systems or networks"(para.1) It is therefore paramount that the management team in the digital libraries put necessary and regular professional information technology training in place to ensure that the loop holes are properly blocked.

In a similar vein, hacking could also be described as sabotage. Sometimes, unwanted and harmful things can be introduced into the computer system through virus and thereby rendering useless the entire resources available in the library. It is important that security measures are put in place to avoid such gaps. Childs (2008) opined that data security should be provided either on-site or off-site and also ensure that a cost-effective solution is provided for target recovery within a short period of time.

It is important to note that there is a slight difference between hacking and cracking. In a situation where hacking is done with harmful intention or motive, it could be referred to as cracking. Dunning (2014) opined that "hackers were programmers who enjoyed the challenge of finding ways to access proprietary computer networks, with no intention of malicious activity"(para.3). People who gain unauthorized access to computer systems with malicious intent should, strictly, be referred to as crackers" (para.3). Similarly, he also observed that there is a term referred to as ethical hacking, which involves "a mutual agreement or term of understanding between a hacker and an organization, which authorizes the hacker to probe, or poke around, in the organization's computer system in an effort to discover sensitive information" (para.3). Ethical hacking is legal.

A proper functioning digital library no matter the size must have a good internet facility. Connections to an external network makes the system a possible target of hackers; it is therefore important that proper traffic monitoring is put in place to watch the network being used in the library (Childs, 2008). The computer engineer or Systems librarian who is saddled with the responsibility of handling and managing the library's servers and systems should be highly competent and over time be trained and retrained. He or she should be willing to learn, unlearn and relearn. The systems librarian cannot do this work solely, therefore it is also necessary that competent systems technicians and assistants are available to assists as the need arises, thereby combating any possible case of hacking.

- **Lack of Data Back - Ups:** Information and resources available in the digital libraries should be regularly 'backed - up' to prevent the case of data loss. A whole library could go down the drain once there is a case of data loss through virus attack or even natural disaster if proper steps were not put in place for back - up. It is usually more professional and safer to make use of automatic back-up system in a digital library. Childs (2008) also noted that back - ups could be created on removable media, even though this could raise security concerns as some unauthorized fellows could take away sizeable quantity of information which sometimes could even be confidential in nature. She therefore reiterated that data security be given high priority and access should be restricted to high capacity media drives and the computer engineer and system librarian should also monitor online data traffic in and out of the library. In the digital library, the use of back - up servers to combat disasters or data loss cannot be ignored. This simply involves the process of cloud computing; that is, storing up data as back - up on a public network to an off-site server (usually located in a different location from the original data). The advantage of this is that in the case of any disaster that led to data loss, the digital library could still have access to the holdings through the data stored up in the back up server; it is also cost effective - storage and infrastructure cost is minimized; Tsagklis (2013) noted that 'it is the biggest advantage of cloud computing, and it is achieved by the elimination of the investment in stand-alone software or servers. By leveraging cloud's capabilities, companies can save on licensing fees and at the same time eliminate overhead charges such as the cost of data storage, software updates and management' (para.2). Another advantage is that it allows for flexibility especially when cloud back - up is being used. The process of remote server back - up should be a routine activity in order to avoid being caught unawares. Despite these advantage of using remote back - up

servers or cloud computing to manage data loss, it is imperative to note that there could also be the challanege of security and privacy in cloud computing. Similarly, Tsagklis (2013) noted that 'cloud based solutions are exposed on the public internet and are thus a more vulnerable target for malicious users and hackers. Nothing on the Internet is completely secure and even the biggest players suffer from serious attacks and security breaches' (para.4). However, despite these challenges, it is still a good means to combat data loss for digital libraries

- **Computer Virus Attack:** This can be described as the introduction of unwanted, harmful, malignant and dangerous programme into a computer system. A computer virus is a written program produced to counter the computer's original program. It also causes damage to both the hardware and software of the computer. ComboFix (2013) observed that "the most potent and vulnerable threat of computer users is virus attacks" (para.1). Combofix also noted that the top sources of virus attacks includes downloadable Programs, cracked software, electronic mail attachments, internet, booting from CD, etc. These harmful viruses usually install themselves onto the computers and spread to the other files on the system, thereby damaging or corrupting the information stored in the computer systems. These computer viral attacks not only pose a threat to the users of the digital library but hamper the process of gaining access to the available resources in the library, which were originally meant to satisfy information needs.

Human Threats

Human threats could also be another source of disaster to digital libraries. Human threat here refers to disaster or damage caused by humans in the digital library systems due to cases of incompetency or sabotage. A single wrong step taken by a technical personnel while handling the equipment in the library could damage the entirety of collections available in the library. Hence human beings (qualified human resources) are seen as important and vital to the proper existence and functioning of a digital library. Apart from natural disasters, all other disasters may be triggered by the actions and inactions of people (employers, employees and outsiders). Human threats may also be considered as malicious threat. Malicious threats can be described as 'insider attacks' planned and executed by disgruntled or malicious employees and 'outsider attacks' maliciously executed by non-employees seeking opportunities to harm and disrupt an organization.

Expectedly,the most dangerous attackers are usually insiders (both current and former employees). This is because insiders in most cases are privy to codes and security measures that are put in place. It is also easy for insiders to perpetuate the malicious plans because they have legitimate access to both the computer and network systems. Employees have access to confidential information, the organization's computers and applications, and they are most likely to know where, how and what to attack that will cause the most damage. Insiders can browse through the file system and plant viruses, trojan horses, or worms.

Institutional Threats

These include mission change, change of legal regime and economic failure.

EFFECTS OF DISASTER IN DIGITAL LIBRARIES

Financial and Economic Implications

Disasters do not only have negative implications for a nation financially, it also affects the corporate organizations and individuals including digital libraries. Sawada and Kotera (2011) observed from their investigations that natural and man-made disasters negatively affect gross domestic product (GDP), which translate into negative per capita consumption level. Furthermore, they found that natural disasters generate the largest negative welfare effects in the short term. Digital libraries located in disaster prone areas, often suffer heavy financial losses. The loss of buildings, infrastructure,

equipment and other facilities can be devastating especially when they are destroyed beyond repair, or when the cost of repairs could carry heavy financial implications. Whether facilities are being replaced or repaired, either way, there are financial implications for losses in digital library disasters. Unfortunately, there are losses that cannot be estimated in financial terms.

Destruction of Physical Equipment and Facilities

The devastating effects of disasters on organizations are mostly felt on building facilities, infrastructure, offices, vehicles and equipment. Digital equipment in the library could be partly or completely damaged if the disaster is caused by floods, earthquakes, fire, bomb blast, chemicals, wars, etc. Recovering, replacing or acquiring new equipments could cause a fortune, especially if there is no disaster management plan in place such as taking insurance against disaster. Insurance is one of the proactive measures digital library managers take to cushion the negative and costly impact/effects of disasters. This is a common precautionary measure in most developed countries and some developing countries. However, many library managers never see the need for this until it becomes too late. In many cases, such libraries never recover from such huge losses and may be faced out of existence. Physical facilities and equipment involve huge capital investments and everything should be done to prevent losing them and the resultant consequencies.

Excess Workload

Apart from the financial costs involved, recovering from disasters could be very tasking to the staff as they would have to work extra hard. They would have to bare overload of work, spending extra time at work or staying beyond the working hours to generate and recreate new data all over again, especially in the library setting. Most times, supervisors assign work targets, stipulating the work to be done and the time frame within which assigned tasks must be completed and so on.

Loss of Personnel

Disasters could trigger the loss of staff. The loss of key management and strategic personnel could devastate the entire library operations. In a situation of disaster, the personnel of a digital library could/may be lost through the following possibilities:

- **Job Loss**: An entire workforce of a library could be layed off and thrown into the labour market, thereby adding to the teeming number of unemployed across the globe. The staff/personnel of a digital library may be dismissed from their jobs if investigations reveal that the disaster was caused by the careless handling of job assignment/responsibility or poor management of the library by the managers. Job loss is much more common in location of wars. People tend to resign from their jobs and relocate if possible for fear of losing their lives, no matter how well paid.
- **Death**: The library could lose her staff in cases of natural or man-made disasters such as earthquake, tsunami, volcanic eruption, hurricane, landslide, bomb blast, and wars/terrorism. The present Syrian civil war has resulted in thousands of deaths including employees of many organizations. According to Anthony (2013), an estimate of about 60, 000 people was reported dead. This estimate rose to about 92, 901 people between 2011 and 2013. The number of deaths certainly will not exclude library personnels working in Syria. Several workers have also died through the deadly activities of Boko Haram in Nigeria. According to Edukugho (2012), more than 4, 000 people have been killed since 2009 as a result of the Boko Haram insurgency. This figure includes military and police personnel and other category of workers in both public and private employment.
- **Physical Injuries and Deformity**: disaster could result in physical damage/deformity to the library personnel's body, such as loss of limbs, and any other part of the body. This means that such library personnel may be retired and if allowed to stay, he/she will no longer be productive. Such a staff may be considered as a loss to the library. Chemical disasters could

result in deformities for a huge number of personnel. So it is important that physical therapists join established programmes rather than attempting individual efforts. In Nigeria, many have been rendered physically deformed as a result of the terrorist activities of Boko Haram. Though, there is no definite record of casualties among the library professionals, there is no doubt that libraries within the locations of Boko Haram's activities in the North East of the country would have been affected.

Psychological Impact

Disaster could also have psychological effects on the staff/personnel. The traumatic impact of an earthquake, landslide, volcano, hurricanes, tsunami, floods, fire, and other disasters could be horrifying to the victims and may destabilize and leave them with mental, emotional and several other psychological problems. The traumatic and emotional toll of disaster on victims is uninmaginable. Some of the common psychological implications of disasters that could affect digital library personnel in a disaster location include: posttraumatic stress disorder (PTSD), depression, insomnia, excessive drinking and smoking and so on. Depression is the second most commonly observed psychological disorders in survivors, followed by various problems with anxiety (Norris, Friedman, Watson, Byrne, Diaz, & Kaniasty, 2002). Across studies, the prevalence of PTSD is higher among direct victims (30-40%) than rescue personnel (20=20%) (Neia, Nandi, & Galea, 2007). Disaster victims have a lot of issues to contend with, which may worsen their situation; issues like relocation, loss of employment, physical injury, legal procedures, and financial loss. These and many other issues are what disaster survivors have to endure.

Disruption of Library Services due to Loss of Reputation

One of the consequences of disaster on a digital library is the fact that the loss of data could also mean loss of customers/patrons and reputation. A digital library that had built a great reputation over a period of time, could suddenly lose her reputation and consequently her patrons as a result of disaster. The teaming customers will have to find another library or other libraries that can render to them the same services and all the resources they need. Disasters destabilizes library processes, operations and services and it will affect the perception and regard patrons have for the library. If patrons perceive that the library can no longer satisfy their information needs, they will definitely look elsewhere and thus, the library will start loosing its reputation. The usual operations and services may be disrupted for a while or permanently, depending on the extent of the damage or impact. Some libraries if they are lucky may still be able to render skeletal services if impact/effect of the disaster was not much. For this category, productivity will definitely decline. Some other libraries may take a while to return to full scale operation of library services, while others may close down permanently.

Disaster and Library Leadership

When disaster occurs, the entire holdings (especially those in digital format) of a library could be destroyed within minutes. The capacity and quality of the library Management are often put to the test during such times of crisis. The actions and inactions of the Management could go a long way in determining the success or failure of disaster management and control. Sometimes the Library Management could be confused and short of ideas, as to how to coordinate other personnel. The decisions made in confusion may worsen the crisis situation.It is better for the Management to hire consultants when they are in doubt of the right steps to take.

Disaster and Loss of Data

Data loss refers to the sudden wiping away of valuable information that has been created and stored over a period of time for specific future use. The effects of loss of data in digital libraries could be enormous. Loss of data where there are no back-up measures can be catastrophic and the consequences are better imagined. The effects of virus on digital resources/collections could become a nightmare

if the necessary precaution was not taken. Recovering certain documents and information may be completely impossible or near impossible if they have not been duplicated in the first place. Some rare documents and grey collections of several centuries back and located only in a specific library may be wiped out.. In other words rare collections that are located in a particular library may be lost forever. These documents could be ongoing research works by academics or scientists that are yet to be completed and published. Other collections could include parchment and scroll materials that have been digitized, including newspapers and book manuscript of many centuries.

ISSUES IN DEVELOPING COUNTRIES

There are salient issues in information and communication technology (ICT) in developing countries that could affect disaster management and control in digital libraries. "Developing country" is a term generally used to describe a nation with low-level material wealth. Levels of development may vary, with some developing countries having high average standards of living (O'Sullivan and Sheffrin 2003). There is high level disparity between developing countries and the developed ones in terms of economic, educational and technological advancements. Developing countries are found in Africa, parts of Asia and South America. This section shall consider ICT disparities and other peculiar issues that could affect disaster management in digital libraries in developing countries.

Digital Divide

The importance of information and communication technology in the economic and industrial evolution of countries in the 21st century cannot be over emphasized. In spite of the influence of ICT on human activities, the relative levels of acquisition and application varies between developing and developed countries. It is this disparity that ushered in the concept of digital divide in the 1990s. Digital divide is simply the worrisome gap that exists between those who acquire and use ICT facilities and those who do not. It is unequal access to ICT facilities such as computers and internet technologies. Warschauer (2002) considered digital polarity as characterized by the under utilization of computers and internet by people of disadvantaged socio-economic background who for various reasons are disconnected from technology resources.

Ogege (2010) posited that digital divide is a multifaceted concept that encompasses global divide (a divide between developing and developed nations) and social divide (a divide between the information rich and information poor within a country). International Telecommunication Union (2005) asserted that the concept of digital divide highlights the uneven distribution process that exists in opportunities to access and use of information and communication technology amongst individuals, households or regions. The divide can either be vertical (the gap between users and non users of information and telecommunication technologies) or horizontal (the gap that exists among users). Cairncross (2001) observed that digital divide is anchored on the inequalities that exist in the growth of and access to information and communication technologies. These inequalities are evaluated through the digital opportunity index. Digital opportunity index is a recognized international information and communication technology indicator developed to measure technological divide among nations. The digital opportunity index sequentially classifies the digital divide into three categories – opportunity, infrastructure and utilization. The opportunity category captures the relative accessibility and affordability of ICTs in a given region or group; the infrastructure category measures the availability of ICT infrastructure; while the utilization category indexes the frequency, quantity and quality of ICT usage. The average ranking (in terms of infrastructure) for developing countries in 2005 was 0.03 (International Telecommunication Union, 2005).

This ranking implies that digital libraries in developing countries are relatively disadvantaged, when compared with their counterparts in the developed world. These disadvantaged libraries lack facilities and personnel to deal with issues and challenges of disaster management. Due to inability to afford and access ICT facilities, most digital libraries in developing countries experience poor response to emergencies and disasters.

Information and Communication Technology (ICT) Policy

A policy framework for information and communication technology is recognized as an important step towards the development of ICTs in any nation. Many developing nations are backwards in ICT advancements due to either lack of or poor implementation of ICT policy framework. These shortcomings affect the provision and management of ICT facilities in organizations including digital libraries. When necessary facilities and an enabling environment are not provided, and in cases where they are provided, they are not well maintained and managed, disasters become inevitable. Achugbue and Akporido (2011) posited that the lack of a coherent policy can contribute to the development (or prolonged existence) of ineffective infrastructure and a waste of resources. They outlined the following as the objectives of ICT policies:

- To increase the benefits derivable from information and communication technology
- Help people and organizations to adapt to new circumstances and provide tools and models to respond rationally to challenges posed by ICT
- Provide information and communication facilities, services and management at a reasonable or reduced cost
- Improve quality of services and products
- Encourage innovations in technology development, use of technology and general work flow
- Promote information sharing, transparency and accountability and reduce bureaucracy within and between organizations and towards the public at large
- Identify priority areas for ICT development (areas that will have the greatest positive impact on programmes, services and customers)
- Attain a specified minimum level of information technology resources for educational institutions and government agencies
- Support the concept of lifelong learning
- Provide citizens with a chance to access information technology resources
- Provide individuals and organizations with a minimum level of ICT knowledge, and the ability to keep it up to date
- Help to understand information technology, its development and its cross-disciplinary impact

An examination of the objectives of ICT polices as enumerated above shows that ICT polices significantly impact disaster prevention, control and management in digital libraries.

DISASTER PLANNING, PREVENTION AND CONTROL IN DIGITAL LIBRARIES

Disaster Planning

Biswas and Choudhuri (2014) opines that disasters have such characteristics as unpredictability, unfamiliarity, speed, urgency, uncertainty and threat. Therefore, efforts should be on prevention and planning before disasters occur and control when they occur. Guha-Sapir, Vos, Below, and Ponserre (2012) stressed that communities, societies, and even nations are not immune to the impacts of disasters. The need for preventive measures and planning has become more apparent especially now that there has been an upsurge in the occurrence of disasters around the world, including highly developed countries like the United States. Between 2001 and 2011, the United States was among the five countries to have experienced the most natural disasters—along with China, the Philippines, India, and Indonesia. These countries are powerful and developed in terms of technology. The fate of developing countries is worse, hence the urgent need for disaster planning in libraries and information centres.

Disaster planning is a matter of basic security for libraries and archives, their staff and their collections. It is considered to be an essential part of any preservation programme to be implemented by any kind of library or archives. A formal written plan enables an institution to respond efficiently

and quickly to an emergency, and to minimize damage to the building and its contents. (Unesco, 2014; and Buchanan,1981)

Australian Library and Information Association (2013) categorically stated that there are two types of libraries or library users in the world - those who have lost data and those who will lose data. Therefore it is essential that Library Management of all types including digital libraries having this important information in mind should make proper plan on how to handle the situation when it happens.

Buchanan, (1988) explained that the decision by any library and any other information centre to undertake disaster planning is very crucial so as to protect collections. He further stressed that disaster occur more frequently in libraries and information centres especially in this digital age and that these disasters result in extensive and costly damage to information resources and services. With the aid of proper disaster planning, these could be prevented or reduced. It is an established fact that the instance of damage to digital collections and equipment in digital libraries is a pointer to the truth that librarians and other information professionals need to initiate disaster planning and make it a major priority for collection and equipment management in digital libraries.

Biswas and Choudhuri (2014) listed five steps that are involved in disaster planning in libraries as follow:

- **Identifying Risks:** the first step is to list geographic and climatic hazards and other risks that could jeopardize the building, collections and services. These might include the institution's susceptibility to natural as well as human made disaster.
- **Decreasing Risks:** The disaster planner should devise a program with concrete goals, identifiable resources, and a schedule of activities for eliminating as many risks as possible
- **Cooperative Plan:** Disaster planning should not take place in a vacuum. To work effectively, it must be integrated into the routine operating procedures of the institution
- **Identifying Resources:** Identify sources of assistance in a disaster. Determine the supplies you will need for disaster response and salvage efforts for your specific collections
- **Setting Priorities:** The first priority in any disaster is human safety while saving collections is the next point of action.

Prevention and Control

It is important for libraries to store patrons data/ information in multiple locations. There is need for at least two data storage locations to safeguard important data including information of users and the collection: The first storage location should be inside the data centre and another outside of the data centre. Duplicate copy should be stored inside the data centre for protection against the loss of individual data server within the syatem. Furthermore, duplicate copies of all data and information should be stored outside the data centre for complete protection against the loss of the data centre. These actions are conducted using procedures that perform data copying between locations. One typical tool for performing this scenario is use of Linux operating systems. (Stević and Kolenkaš, 2014)

Australian Library and Information Association (2013) noted that digital library software can be set to capture an image of a library's system every 15 minutes, so data need never be exposed to more than 15 minutes of risk. Software then uses the captured image to migrate data back to the same piece of hardware, on the premise that the machine is operational, otherwise to a new server once one has been sourced. Using modern technology, it only takes about ten minutes to migrate the old data to a new server, regardless of size. Early detection of possible problems is another method of preventing disaster in digital libraries. Some Software now allows an information technology manager / staff or digital librarian as the case may be, to view a server's performance from a remote location, to ensure that the library's hardware is running well and back-ups are being performed on schedule so as to prevent the server from possible damage and the resultant consequence of data loss.

Another method of preventing or controlling disaster in digital libraries is ensuring that data and information on servers are backed - up remotely and virtually. Cloud computing storage solutions now have the ability to restore files and folders to be restored locally or remotely in a fraction of the time of a traditional backup product. An entire computer infrastructure can be spun up to full production in minutes. (Australian Library and Information Association 2013). Ensuring computer, data and information security must be an integral put of any disaster plan in digital libraries.

Computer and Information Security

Computer security implies all legitimate means used to prevent and detect unauthorised access to a computer network.It has now be extended to include securing privacy, confidentiality and integrity of data and information on a network. This is particularly important for digital libraries if they must prevent virus attacks, hacking and cracking related disasters. Protective measures involved in computer security include the following:

- **Prevention:** Take appropriate precautions that could prevent important data and information from being damaged, altered, or stolen. These measures could range from ensuring that the door to the server room is locked to setting up and implementing high-level security policies.
- **Detection:** Put in place necessary measures that allow the library to detect information damage, alteration, or theft. The library should also be able to promptly determine the level of data and information damage, alteration, or theft and accosting persons responsible for the damage.
- **Reaction:** Take Prompt steps to recover information, even if information is lost or damaged.

Discussion on prevention of disaster in digital library will not be complete without the mention of some salient issues that should be of utmost importance and consideration to digital library management in developing countries.

1. **Information:** The difference between the developed and developing countries can be attributed to the amount of information available for their utilization. Information plays critical role in decision making; it enables the organization or library to know what to do and how to do it. Therefore, digital library management should source for information on best practices in the management and prevention of disasters in their organizations.
2. **Learning from the Experience of Others:** Disaster has occurred in digital libraries over time. It is only logical for Digital Library Managers who want to prevent disasters from their own libraries to as a matter of necessity learn from the experience of those who had passed through it. This can help Library Managers to be abreast with the rudiments and essentials of disaster prevention and control. It is better to learn from the mistakes of others, than to face the consequence of a disaster .
3. **Digital Library Resources:** The standard of the resources in digital library will have direct impact on its functionality. Resources in digital library in this regard refer to human and equipment.The human resources in digital library are the manpower that manage the library. In actual fact, the manpower in digital library directly or indirectly affect the standard and service of the library. In the event that unqualified and inexperienced Library Staff are employed to manage the library computer network (hardware ad software), the probability of a disaster becomes higher. This is most prevalent in developing countries. In the same vein, the quality of equipment used in a digital library will have effects on its functionality. Acquisition and use of substandard equipment in the library will definitely lead to disaster. Sometimes, the temptation to acquire substandard equipment is high, as such equipment are usually cheaper. Library Managers who are more interested in saving cost, rather than performance and excellence go for such substandard equipment. The final outcome of such poor decisions are the occurrence of preventable disasters. Cheaper computer

sets, application software and other network facilities may increase the chance of disaster and data lost in digital libraries.

4. **Maintenance Culture:** Most developing countries and their libraries lack maintenance culture and this can result to disaster in digital library. The equipment in digital library need routine checks and maintenance. This will help to detect, service and repair or replaced faulty parts before they cause disasters.
5. **Incessant Power-Outage:** The rate at which most developing countries experience power outages call for a rethink. Incessant power outages and the resultant surges could trigger fire outbreaks that could lead to disasters.Sometimes, computer systems and other network facilities are outrightly destroyed by sudden electricity upsurge occasioned by incessant power flunctuations and outages. Ensuring stable power supply must be embedded in the disaster plan for digital libraries.

It is encouraging to note that some hybrid libraries (libraries that combine traditional and digital methods in their operations and services) in Africa have taken appropriate steps to prevent disasters to their digital collections,through the adoption of the cloud computing model (Ifijeh, 2014). Notable among these are the libraries of Covenant University, Nigeria, University of Legon, Accra, Ghana, University of Botswana, and some Universities in South Africa among others.

Further Recommendations For Developing Countries

Because of the fact that disaster is unpredictable and its effects are catastrophic, it is recommended that:

- **Digital Libraries Should have a Written Disaster Plan:** This will serve as a guide on what to do and how to prevent and control disaster, and in the event of its occurrence, the plan outlines what steps to follow so as to immediately restore library operations and services as well as recover any loss data.
- **Employment of Competent Human Resources to Manage the Digital Library:** It is believed that people are the most valuable asset to any organization. it is therefore essential that the right caliber of staff in the right mixes both in quality and quantity should be employed to manage the digital library so as to prevent and control disasters.
- **Digital Libraries Should Acquire Quality Equipment for Effective and Efficient Operations of the System:** Sub-standard equipment do result to disaster in the long run. Efforts must therefore be made to ensure that equipment, facilities and materials of the highest quality and standard are procured in digital libraries. There should be good and reliable back - up systems for data. The back - up systems should be kept in different locations, within and outside the library. There is need for cloud back-up for recovery of data in the event of disasters.
- **Protection of Digital Library Server Against Hackers and Virus:** Hackers and virus attacks are dangerous agents of distraction and major causes of disaster (mainly leading to data corruption and lost) in digital libraries. Management of digital libraries should put anti-intuitions mechanisms in place so as to minimize (if not prevent) hackers and virus access to the digital library server.
- **Training and Development:** The importance of training and development cannot be over emphasized. There is need for regular training of manpower working in the digital library. They need to be trained and retrained by their parent organizations through conferences, seminars, workshops and so on. This will give them the opportunity to learn current trends in their field and apply same for the advancement of the digital library; this will reduce the risk of disasters in digital libraries.

CONCLUSION

The applications and proliferation of information and communication technology (ICT), as well as the increases in digital transactions and communications in libraries, have created new opportunities and greater access to information resources for library users. ICTs have opened new windows which have resulted in the emergence of digital libraries. This article has focused on disaster management in digital libraries. It discussed an overview of the concept of 'digital library' and examined the causes, effects, prevention and control of disasters in digital libraries. It also covered some salient issues relating to disaster management in developing countries. Thus, digital divide and lack of national ICT policy framework, were identified as critical issues that must be resolved in developing countries if disasters must be prevented and properly managed in digital libraries.

Just as it is with conventional libraries, digital libraries will continually be faced with threats of disasters; while it may be possible to prevent some disasters, their occurrence cannot be totally ruled out, because both the humans and machines that operate the systems are prone to weaknesses, errors and aberrations. One can only hope that with better policies put in place, more funds made available and judiciously used, employment of qualified personnel and visionary leadership, occurrence of disasters in digital libraries would become minimal in developing countries. It is also hoped that policy formulators and implementers would adopt the recommendations made in this article.

REFERENCES

Achugbue, E., & Akporido, C. E. (2011). National Information and Communication Technology Policy Process in Developing Countries. In E. Adomi (Ed.), *Frameworks for ICT Policy* (pp. 107–123). Hershey, PA: Information Science Reference (an imprint of IGI Global). doi:10.4018/978-1-61692-012-8.ch014

Altman, M., Adams, M., Crabtree, J., Donakowski, D., Maynard, M., Pienta, A., & Young, C. (2009). Digital Preservation through Archival Collaboration: The Data Preservation Alliance for the Social Sciences. *The American Archivist*, *72*(1), 170–184. doi:10.17723/aarc.72.1.eu7252lhnrp7h188

Anderson, C. (2005). Digital Preservation: Will your Files Stand the Test of Time? *Library Hi Tech News*, *22*(6), 9–10. doi:10.1108/07419050510620226

Anthony, H. C. (2013). *The Human Cost of the Syrian Civil War*. Retrieved from http://csis.org/publication/human-cost-syrian-civil-war

IT Disaster Recovery. November/December 2013 INCITE. (2013). Australian Library & Information Association. Retrieved from https://www.alia.org.au/sites/default/files/publishing/INCITE_web34.3.pdf

Biswas, B. C., & Choudhuri, S. K. (2014). Digital Information Resources for Disaster Management of Libraries and Information Centres. *Bangladesh Journal of Library and Information Science*, *2*(1), 12–21.

Buchanan, S. (1981). Disaster, Prevention, Preparedness and Action, Library Trends. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.173.5974&rep=rep1&type=pdf

Buchanan, S. A. (1988). Disaster Planning: Preparedness and Recovery for Libraries and Archival. Retrieved from http://eric.ed.gov/?id=ED297769

Building Digital Bridges. (2005International Telecommunication Union, International Telecommunication Bulletin, Geneva.

Cairncross, F. (2001). *The Death of Distance: How Communication Revolution is changing our Lives*. Boston: Howard Business School Press.

Cervone, H. F. (2006). Disaster Recovery and Continuity Planning for Digital Library System. OCLC Systems and Services. *International Digital Library Perspectives.*, *22*(3), 173–178. doi:10.1108/10650750610686234

Childs, D. R. (2008). *Prepare for the Worst, Plan for the Best: Disaster Preparedness and Recovery for Small Businesses* (2nd ed.). New Jersey: John Wiley & Sons.

Top 5 Sources of Computer Virus Attack. (2013). *ComboFix*. Retrieved from http://www.combofix.org/top-5-sources-of-computer-virus-attack.php

Dunning, D. (2014). What Is the Definition of Computer Hacking. *eHow Technology Electronics*. Retrieved from http://www.ehow.com/info_8642666_definition-computer-hacking.html

Edukugho, E. (2012). Boko Haram: Tallying Casualties of the Insurgency. *Vanguardngr.com*. Retrieved from http://www.vanguardngr.com/2012/12/boko-haram-tallying-casualties-of-the-insurgency/

Guha-Sapir, D., Vos, F., Below, R., & Ponserre, S. (2012). Annual Disaster Statistical Review 2011: The Numbers and Trends. Centre for Research on the Epidemiology of Disasters, Brussels. Retrieved from cred.be/sites/default/files/2012.07.05.ADSR_2011.pdf

Ifijeh, G. (2014). Adoption of Digital Preservation Methods for Theses in Nigerian Academic Libraries: Applications and Implications. *Journal of Academic Librarianship*, *40*(3-4), 399–404. doi:10.1016/j.acalib.2014.06.008

Neria, Y., Nandi, A., & Galea, S. (2007). Post-traumatic stress disorder following disasters: A systematic review. *Psychological Medicine*, *38*(4), 467–480. PMID:17803838

Norris, F. H., Friedman, M. J., Watson, P. J., Byrne, C. M., Diaz, E., & Kaniasty, K. (2002). 60,000 disaster victims speak: Part I. An empirical review of the empirical literature, 1981-2001. *Psychiatry*, *65*(3), 207–239. doi:10.1521/psyc.65.3.207.20173 PMID:12405079

Nwalo, K. I. N. (2011): New Mode of Universal Access: Challenge to Nigerian Cataloguers. *Paper Presented at the 31st Annual Seminar/Workshop of the Nigerian Library Association* (pp. 30-38).

O'Sullivan, A., & Sheffrin. (2003). *Economics: Principles in Action*. Upper Saddle River, NJ: Pearson Prentice Hall.

Ogege, S. O. (2010). *Nigeria's Development Challenges in a Digitalized Global Economy. African Research Review*, *4*(4), 111–122.

Ottong, E.J., & Ottong, U.J. (2013) Disaster Management of Library Materials in Federal Universities in Cross River and Akwa Ibom State, Nigeria. *International Journal of Educational Research and Development*. 2(4), 98-104.

Sawada, Y., & And Kotera, T. (2011). Disasters and Economies. *World Economic Review*, *55*(4), 45–49.

Stević, M. P., & Kolenkaš, I. Ž. (2014). Enabling Disaster Recovery Scenario in Digital Libraries Using Eventual Consistency. *Online Journal of Applied Knowledge Management.*2 (2), 57 – 67. Retrieved from http://www.iiakm.org/ojakm/articles/2014/volume2_2/OJAKM_Volume2_2pp57-67.pdf

Tsagklis, I. (2013). Advantages and Disadvantages of Cloud Computing- Cloud Computing Pros and Cons. *Java Code Geeks*. Retrieved from http://www.javacodegeeks.com/2013/04/advantages-and-disadvantages-of-cloud-computing-cloud-computing-pros-and-cons.html

Disaster Planning Prevention, Preparedness, Response, Recovery. (2014). *UNESCO*. Retrieved from http://webworld.unesco.org/safeguarding/en/pdf/txt_sini.pdf

Warschauer, M. (2002) Reconceptualizing the Digital Divide. Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/967/888/

Goodluck Ifijeh is a Serials Librarian (Newspapers) at Centre for Learning Resources, Covenant University, Ota, Nigeria. He obtained an MLIS degree from the University of Ibadan in 2011 and has made numerous contributions in journals and books.

Jerome Idiegbeyan-Ose is the Head, Technical Services, at the Centre for Learning Resources, Covenant University, Ota, Nigeria. He is currently a doctoral student at Babcock University, Nigeria. He has published articles in local and international journals, as well as chapters in books.

Chidi Segun-Adeniran works in the technical services unit of the Centre for Learning Resources, Covenant University, Ota, Nigeria. She holds both BLIS (first class division) and MLIS from the University of Ibadan, Nigeria. She has made contributions in journals and books.

Julie Ilogho is Serials Librarian (Journals) at Centre for Learning Resources, Covenant University, Nigeria. She is currently a doctoral student and has published numerous articles in journals.