Vulnerabilities Facing Digital Content at the University of Nairobi and Catholic University of Eastern Africa Academic Libraries

David S. Chickombe* Charles Maina
Kenyatta University

Abstract

An academic library is a library that is attached to a higher education institution and serves two complementary purposes: to support the curriculum, and to support research by university faculty and students. Increasingly, these very sacrosanct information centres to the University mandate are faced with security threats on digital content. These threats include but are not limited to computer-assisted fraud, espionage, sabotage and vandalism. The study objective of this study was to examine the vulnerabilities facing digital content at the University of Nairobi and Catholic University of Eastern Africa academic libraries. The study employed a descriptive survey design. The target population in this study were 2 Information and Communications Technology Managers and 10 ICT technicians, 2 Chief Librarian and 20 Library Staff. The study had a target population of 34 respondents. A census was used to arrive at a sample of 34 respondents from the two university academic libraries. Data was collected by use of semi-structured questionnaires, with both closed and open ended questions. The quantitative data analysis was conducted using descriptive statistics to obtain frequencies and percentages. The key findings of the study are that the university lack proper disaster management on digital content information materials. There is Lack of reliable infrastructure and resources in the library, lack of enough funding and sometimes delayed provision of funds for procurement of necessary computing equipment thus hindering the establishment of disaster recovery centres, lack of programmes to guide on training and training needs, unclear policies and guidelines in the University. The study provides several recommendations that would improve the current state of disaster planning and preparedness. The university should train and retrain its core staff to ensure that they are updated with current knowledge and skills that focuses on ever changing security threats to digital security and preparedness. The institutions management should give provision of adequate funds for continuous training. The institution should have policies to guide on passwords, privileges and have disaster recovery procedure and universities should explore more methods of ensuring Security of digital contents.

Keywords: Academic libraries, Vulnerabilities, Digital content, University of Nairobi, Catholic University of Eastern Africa
DOI: 10.7176/IKM/11-4-02
Publication date: May 31st 2021

Introduction

The primary obligation of any academic library is to meet the information needs of its members. To do this end, libraries have introduced network services such as internet, electronic journal services, web Online Public Access Catalogue (OPAC), CD ROM searching services, and digital collections among others Khan M. A. (2013). This has become very important especially with the introduction of distance, open and e-learning programmes in institutions of higher learning. The introduction of these programmes calls for a 24/7 access to information resources. The automated services help in providing equitable levels of service across the whole institution including distant users. It is therefore, important to ensure that these services are made available to clients whenever needed. However, digital contents are prone to various kinds of man-made or natural threats or disruptions such as denial of access to information that may lead disorganization of the academic calendar Njoroge, (2014).

Ifijeh, Idiegbeyan-Ose, Segun-Adeniran, and Ilogho (2018) stated that despite the advantages derived in the use of automated methods in carrying out library and information services, the occurrence of disasters for digital content cannot 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" Disasters could be linked to physical, environmental and technological factors such as explosion, loss of power, internet failure, flood and cyber-criminal activities etc. The advent of digital content has increased the occurrence of disasters caused by technical and technological factors. These could include hampering of e-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.

Digital disasters can occur in parallel with natural or man-made disasters or can happen of their own accord. The status of digital content and preparedness on disaster recovery measures taken by libraries in China were studied by Jiazhen and Daoling (2007). Findings indicated that physical deterioration of data led to non-renewable data loss, inability to read the data due to obsolete storage media, weak data back-up management system, shortage of relevant knowledge on preserving digital information resources and failure to migrate the obsolete data in time.

A comparative evaluation among three main cultural institutions in Malaysia regarding long term preservation of digital content is presented by Manaf and Ismail (2010). To avoid digital disaster, issues relating to hardware and software compatibility, long-term storage, organization of files for ease of search and retrieval, media quality, disaster recovery and integrity of original data have to be kept in mind.

Hawkins et al. (2000) studied digital content preparedness in India and highlighted issues related to preparedness and recovery from digital disasters. The authors explain the need to have a disaster recovery plan and discuss how to cost it. They also stress the issue of insurance and training of human beings. Tennant (2001) describes how to cope with disasters in digital libraries and what preparation measures should be taken to avoid disasters. Boss (2002) also explains how a proxy-server and firewalls can protect the database server of a library. Georges (2004), emphasizes issues related to having properly trained staff, types of servers to have, backup of data, damage assessment and recovery and restoring operations.

A survey of the preparedness for digital preservation of Local Authority Archives in the United Kingdom was conducted by Boyle, Eveleigh, and Needham (2008) where over 80 percent of the respondents already held digital collections. Preparedness for digital preservation was assessed in terms of digital preservation planning, general awareness of digital preservation, current practical digital preservation strategies, infrastructure and staffing requirements. The results indicated that awareness of essential issues of digital curation and preservation was particularly low in those organizations without a preservation policy. In the same study, barriers to digital curation and preservation were identified as cultural (organization, political, awareness, external partnerships/relations and motivation), resources (time, costs, funding and storage), and skills gap training, competencies and information technology (Ndhlovu and Matingwina, 2016).

In Africa, Miller and Blake, (2011) research stated that libraries may manage digital content in three primary ways; providing access to metadata and electronic full-text for publisher or vendor content, managing digitized local collections, and managing institutional, scholarly digital assets. The researchers work at the National University of Science and Technology (NUST) Library in Zimbabwe observed that the library has embraced the practice of e-collection and digitization by establishing a number of digital collections in order to meet the demands of the 21st century clientele. As a result, the library has amassed a large body of valuable digital assets and information which include among other things institutional records, faculty and student research, theses and dissertations, university publications, past examination papers, multimedia collections and course materials.

In Kenya, Wambiri (2008) studied disaster management for university libraries that focused on general disasters that could occur in a library. Kimani and Muthembwa (1998) also studied general disasters that occur in libraries and not those specific to digital library or content. Methods used to prevent and prepare for a disaster in a traditional library and its systems may be different from those used for digital. There exists a gap in knowledge on disaster management for digital content in libraries in institutions of higher learning in Kenya. It is in this light that this study will focus on disaster preparedness systems that include preparedness for digital content in selected academic libraries of University of Nairobi (UoN) and Catholic University of Eastern Africa. A quick search through the websites of universities in Kenya and websites of their respective libraries indicated that all university libraries were automated.

Statement of the problem

Cervone (2006) points out that disaster recovery planning and business continuity planning are two of the most critical components of the digital library system infrastructure, yet they are aspects that are often overlooked. The neglect of digital content is unfortunate because the consequences of being unprepared for disaster are significant. A week long power failure in 1998 seriously impacted services of the 13 libraries on the campus of the University of Auckland, New Zealand (Grant, 2000). After an AC outage, the server of Montclair University Library did not restart as the aging server equipment did not have automatic temperature control, no documentation was done for restoration of system, and no testing of restoration of data backup was done (Mallery, 2012).

University libraries in Kenya have increasingly continued to automate services in a bid to effectively and efficiently meet the information needs of their students, lecturers and researchers (Njoroge, 2015). A library, being the heart of any learning institution, is strategic in meeting its clients' learning, teaching and research objectives. Any interruption or failure that will interrupt service flow will cause devastating effects to the overall information dissemination to the entire university clientele spectrum.

However, studies to ascertain the state of digital content disaster preparedness for academic libraries in Kenya have been broad, focusing on the general disaster preparedness (Wambiri 2014) and (Njoroge 2015) recommending more research in this area of study while specific research on digital content vulnerability risk management is still in its infancy stage and hardly available in the existing literature in the selected universities.

It is within this context; that the study seeks to explore the digital content vulnerability risk management at the selected Universities in a bid to create a proactive approach to formulate policies and test, prepare budgets and human resources to be able to adequately face and handle software contents vulnerabilities in academic libraries.

Significance of the Study

The study findings could be used to make policy decisions on disaster management for CBIS by university management, government stakeholders such as Commission for University Education, government ministries such as Ministry of Education, Science and Technology, Ministry of Information and Communication Technology, among others.

The study findings will contribute to knowledge on the topic of the digital content vulnerability continuous research.

LITERATURE REVIEW

The Internet is the world's greatest network as it is the driving force behind globalization and modern progress, it has enabled people to communicate with others across the world almost instantly and provides a medium for cultural, informational, and ideological exchange. It also provides a previously unimaginable level of interconnectedness that benefits business, government, and civilians alike. But for all the good that comes from the Internet, this "series of tubes," as described by Senator Ted Stephens, can be used for more nefarious purposes, Vermaaten S, (2012). Vermaaten, further asserts that, while the Internet affords people living in starkly different circumstances around the world access to the same information, it also acts as an equalizer between governments and non-state actors. People now live in a world where government databases and public utilities can be invaded and disrupted by advanced attacks launched by foreign governments; computer-literate teenagers bored during Covid-19 lockdown; or even a single man working from his balcony.

According to Patel, Qassim, & Wills. (2010), in this information age, through internet, millions of users access and exchange lots of data/information content in complex work flow processes. This is attributted to information sharing having been made easier and less expensive by internet technologies and global networking infrustracture, but availability of such information systems comes with higher risks. Due to cybercrime, before long, information if not preserved, websites tend to disappear frequently and digital media become obsolete easily and there could be an abuse on the privacy of information, moreover, the integrity of the systems could be compromised. The integrity and availability of all these systems have to be protected always against a number of threats. Hackers, rival corporations, terorrists and even government agencies have the motive and capability to carry out sophisticated attacks against computer systems (Patel, et al,2010). Thus , security mechanisms appropriate for internet based, real worlds applications should be a prerequisite in all digital setups and maintenance.

It is not lost from observers that the manner in which institutions charged with the responsibilities of providing help to victims of terror and natural calamities that have occurred in some parts of the world have clearly shown inadequate professional disaster preparedness. Despite the increasing investment in information security and its strategic role in today's business success, effective implementation of information security strategy still remains one of the top challenges facing global organizations (Fratto, 2009; Price water house Coopers 2008. Businesses are being urged to make information security, a strategic issue for organizations "e-library" to compete and survive in this era of global economy and ever changing enterprise risks (Amano, 2009).

There are numerous threats that deal with the whole concept of security in libraries, but for the sake of this study, there are only four main streams that concerns security in the digital environment namely: Infrastructure; digital content; user information security; and lastly standards and legal issues.

Infrastructure

From study findings by Lampson (2004), it emerged that people have been working on computer system security for more than three decades and have registered notable intellectual success. But despite this, still the security risk of millions of deployed computer systems is so high that a determined and competent attacker could destroy most of the information on almost any of the systems or steal it from any system that is connected to a network or even attack millions of systems at once.

According to Zimerman, (2009), library computers are not safe, as they are physically vulnerable to theft, damage and destruction, but, most of all, they are vulnerable to attacks by a host of malware agents which include Trojans, viruses, worms, adware, spyware, pornware, keystroke loggers, password stealers and others. It worthy to note that hackers, viruses, worms, and trojan horses are external extrusions which well-established libraries should be able to handle, Al- Suqri & Afzal, (2007). Despite there being antivirus software's which are popular, it has been established that they are not the ultimate protection but instead more dangerous. There are cyber criminals who specialize in targeted attacks, making it more difficult to handle the risk with the traditional antivirus systems asserts Zimerman, (2009). And given the value of information that digital libraries hold, they have a cause to worry about this problem. This creates a danger, which is a multifaceted threat facing every computing environment, despite there being protection systems that can be applied but some are too expensive for a library and they only help to minimize but are never perfect (Zimerman, 2009).

Digital Security Threats

Every organization should be at the forefront of change processes. Where continuous information is available, reliability and time is a key advantage. The threats to the network security are not just for organizations, but can be observed all over the world in different countries and the degree to which each of them are exposed to the threats. The statistics to which can be seen in the table illustrated below:

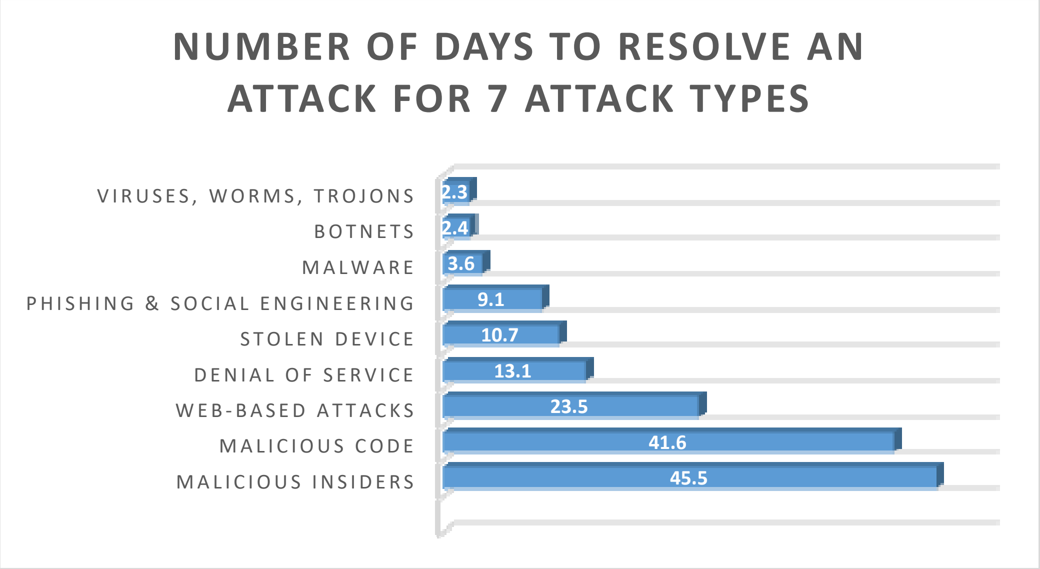

Figure 1. Number of days taken to resolve an attack by type of attack types.
Source: Serianu Cybercrime Security report 2018

Information Threats

The latter are always a combination of tools that have to do with technology and human resources (policies, training). Attacks can serve several purposes including fraud, extortion, data theft, revenge or simply the challenge of penetrating a system. This can be done by internal employees who abuse their access permissions, or by external attackers to remotely access or intercept network traffic.
There are several types of digital security threats as enlisted here below:

Web Application Level Vulnerabilities

Despite the laws in European countries that mandate secure sites, many library websites have serious security flaws which render then vulnerable to attacks (Kuzma, 2010). From a research conducted in European countries, almost 80 percent of web related flaws were caused by web application vulnerabilities with the three main common types being: Cross scripting, Denial of Service and SQL injection. Major causes for these problems are pointed to be, lack of updating software versions, developers install the default software and forget the need to update, lack of consideration of security flaws, lack of upgrading software correctly and lack of effecting coding practice during designing and development states, Kuzma, (2010).

RESEARCH METHODOLOGY

The study adopted a descriptive survey research design. The study was carried out in Nairobi County, where both University of Nairobi and the Catholic University of Eastern Africa academic libraries are located. The target population for this study was library employees and ICT professionals in charge of library ICT infrastructure at the two institutions of higher learning. The population was stratified into two strata namely library professionals and ICT professionals. The sample for this study was selected through convenient sampling method. A total of 34 respondents (as shown in table 2) were sampled from both the Library professionals and the ICT professionals.

Table 1. Sampling frame of Target population.

Category	Chief Librarian	Library Staff	ICT Manager	ICT technicians	Total
UoN	1	11	1	5	18
CUEA	1	9	1	5	16
Total	2	20	2	10	34

A sample of 34 respondents was selected Herzog, Scheuren and Winkler, (2010) asserts that a census is a study that obtains data from every member of a population. A census is only practical where the target population is small and there is a high probability of getting more information by targeting the entire population. Primary data was collected through semi-structured questionnaires.

FINDINGS

Demographic distribution of respondents

Table 2: Demographic distribution of respondents presents demographic information of the respondents.

Table 4.1 Distribution of Demographic Information of Respondents			
Variable		**Frequency**	**Percentage (%)**
Age	20-25	7	25
	31-35	3	10.7
	36-40	2	7.1
	41-45	9	32.1
	above 45	7	25
Total		**28**	**100**
Gender distribution table 4.1 (b)			
	Gender	**Frequency**	**%**
Gender	Male	16	57.1
	Female	12	42.9
Total		28	100
Intervening profession distribution table (c)			
		Frequency	**%**
Designation	ICT Manager	3	10.7
	Librarian	15	53.6
	Network Manager	10	35.7
Total		28	100

The data presented in Table 2 shows that by age, 9(32.0%) were within the age bracket of 41-45 years, 7(25.0%) of the respondents were above 45 years, 3(10.7%) within 31-35 years while 2(7.1%) were within the range of 36-40 years.

In terms of gender of respondents 16(57.1%) were males while 12(42.9%) were females. These percentages are in line with the current gender policy in the Republic of Kenya, as the female respondents have more than 30% representation in the study.

Concerning the designation, majority of the respondents 15(53.6%) were librarians, 10(35.7%) were network managers while 3(10.7%) were ICT managers.

Disasters Experienced

The study sought to find out if the universities had ever experienced any disaster in their libraries, all the respondents agreed that they have experienced disasters in the universities. The respondents stated that there have been computer viruses in the digital library which at one time left the feeling of helplessness in work at the university was brought to a halt for a period of 3 days. This was restored back after the Information Technology (IT) department worked tireless by use of different anti- viruse software in all the digital library machines. Another disaster that was mentioned was theft of information materials (78.0%) water leaking pipes (22.0%) as other threats within the academic libraries.

Digital content vulnerability disaster preparedness.

In relation to implementation of the digital disaster preparedness in the Universities, the respondents were asked whether their library has implemented the digital disaster preparedness. Results are indicated in figure 2 below.

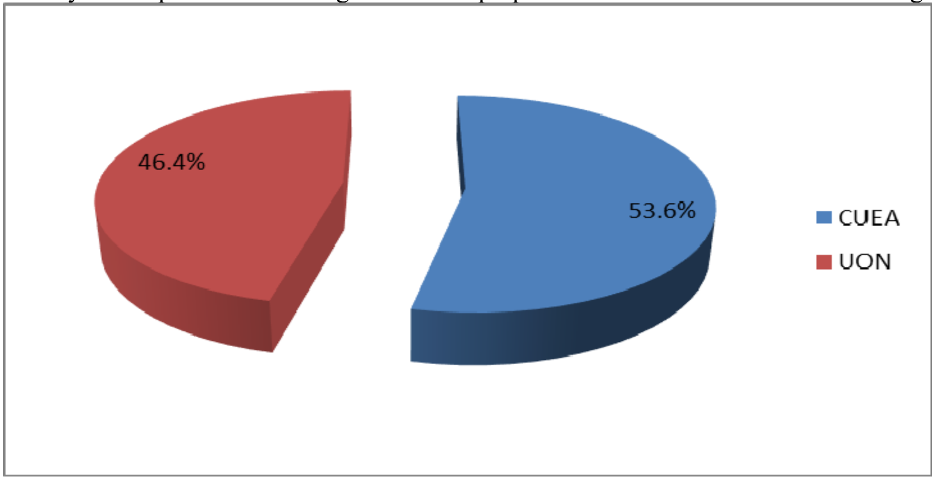

Figure 2: Library implemented the digital disaster preparedness plan

From figure 2, 15(53.6%) of the respondents agreed that they had implemented the digital disaster preparedness in their institutions while 13(46.4%) disagreed that they had implemented the digital disaster preparedness.

Digital security threats faced by management of libraries in your institution.

Table 3 Digital security threats faced by libraries

Statement	**SA**		**A**		**N**		**D**		**SD**	
	Freq.	%	Freq.	%	Freq.	%	Freq.	%	Freq.	%
Library databases are vulnerable to attacks launched by detractors,	18	64.3	5	17.9	2	7.1	2	7.1	1	3.6
Information is not well preserved, websites tend to disappear	17	60.7	0	0	5	17.9	2	7.1	4	14.3
Our library has the prerequisite security mechanisms.	2	7.1	0	0	7	25.0	0	0	19	67.8
Computers are not safe, as they are physically vulnerable to theft, damage	14	50.0	9	32.1	2	7.1	1	3.6	0	0
There is all-inclusive committee charged with the task of mitigating disaster that may affect institution.	2	7.1	0	0	0	0	22	78.6	4	14.2
management has in place adequate security measures to respond to cybercrime at the shortest time possible.	0	0	0	0	4	14.3	4	14.3	20	73.4
Both students and staff have the knowledge of responding to cases of cyber threats.	8	28.2	10	35.7	0	0	0	0	10	35.7
Our library having antivirus software's they are more dangerous.	11	39.3	6	21.4	0	0	10	35.7	0	0
Websites have serious security flaws which render them vulnerable	19	67.9	4	14.3			2	7.1	3	10.7

Source Researcher September 2020.

Results from table 4.3, 18(64.3%) of the respondents strongly agreed that library databases were vulnerable to attacks launched by detractors, through hacking, worms or viruses, 5(17.9%) agreed, while 3(10.7%) disagreed.

Most the respondents 17(60.7%) strongly agreed that information in the university libraries is not well preserved making websites to disappear frequently and digital media becoming obsolete easily, 5(17.9%) were neutral (not sure if information is not well preserved or not), 4(14%) strongly disagreed while only 2(7.1%) disagreeed.

A good number of respondents from UON and CUAE universities strongly disagreed 19(67.8%) that the university libraries had the prerequisite security mechanisms appropriate for internet based, applications in all its digital setups and maintenance, 7(25.0%) were neutral while 2(7.1%) strongly agreed that there were security mechanisms appropriate for internet baseda pplications in all its digital setups and maintenance.

The findings indicated that 14(50.0%) strongly agreed that library computers are not safe, as they are physically vulnerable to theft, damage and destruction, but, most of all, they are vulnerable to attacks by external threats, 9(32.1%) agreed, 2(3.6%) while 1(3.6%) disagreed.

On finding out if universities had in place an all-inclusive committee that is charged with the task of mitigating any disaster that may affect our institution, 22(78.6%) disagreed, 4(14.2%) strongly disagreed while 2(7.1%) strongly agreed that there was a committee.

Majority of the respondents 20(73.4%) strongly disagreed that the University management has in place adequate security measures to respond to cybercrime at the shortest time possible, 4(14.3%) disagreed while 4(14.3%) were not sure if there were security measures in place or not.

Further on finding out from the respondents if both students and staff from the institutions had knowledge of responding to cases of cyber threats, 10(35.7%) agreed to it, 8(28.2%) strongly agreed that they had knowledge while 10 (35.7%) strongly disagreed. On probing further, the respondents indicated that though they had training on to respond to cases of cyber threats they haven't put it into practice at the university due to lack of implementation of what have been impacted during trainings.

It is indicated that though the University library having antivirus software's which are popular, they are not the ultimate protection but instead more dangerous, with 11(39.3%) strongly agreeing to it, 6(21.4%) agreed, 10(35.7%) strongly disagreed, implying that antiviruses that have been installed in libraries have no ultimate protection thus being dangerous to the library information.

As for the institution library websites having serious security flaws which render them vulnerable to attacks majority of the respondents 19(67.9%) strongly agreed, 4(14.3%) agreed, 3(10.7%) strongly disagreed while 2(7.1%) disagreed showing that universities have serious security flaws rendering the libraries vulnerable to attacks.

Discussions of Findings

The respondents agreed that they had experienced disasters in the institutions related to information security at the respective libraries. There have been computer viruses in the digital library which left the feeling of helplessness among the library and students at the university thus bringing to a halt a period of 3 days. Another disaster that was mentioned was theft of information materials (78.0%). CUEA University by taking it seriously to acquire and install the necessary softwares, and acquire relevant IT licenses. Develop relevant policies and invest adequate finances to support cyber security.

The findings showed that cybercrime has posed to the great extent on the smooth running of the two university libraries, respondents agreed that library databases of the universities were vulnerable to attacks launched by detractors, through hacking, worms or viruses. It was strongly felt that information in the university libraries was not well preserved making websites to disappear frequently and digital media becoming obsolete easily. Respondents observed that the university libraries didn't have the prerequisite security mechanisms appropriate for internet based, applications in all its digital setups and maintenance (67.8%).

Further, respondents indicated that library computers were not safe (50.0%), as they are physically vulnerable to theft, damage and destruction, but, most of all, they are vulnerable to attacks by external threats via the internet. The two universities did not have an all-inclusive committee charged with the task of mitigating any disaster to digital content that may affect the institutions (78.6%), making the library very vulnerable to attacks.

The University management also lacked aadequate security measures to respond to cybercrime at the shortest time possible. In any institution securing a computer-based information system is coming up with controls as mechanisms to reduce or clear digital content threats to network security (Fitzgerald and Dennis, 2002). There are three main types of controls that prevent, detect and correct whatever might happen to the organization through the threat faced by its computer-based systems.

Having adequate and trained employees' plays a very significant role in any institution. Lack of training will always hamper the smooth running of any institution. In the two targeted universities there was lack of knowledge of responding to cases of cyber threats, though employees had training on responding to cases of cyber threats they haven't put it into practice at the university due to lack of implementation and resources of what have been impacted during trainings.

It was indicated by the respondents that though the University library had antivirus software which were popular, they were not the ultimate protection but instead were more dangerous. This implied that antiviruses that have been installed in libraries have not provided the much needed protection to library digital content thus, posing more threats to library digital information. The library websites had serious security flaws which rendered them vulnerable (67.9%).

Conclusions

The study established that the two academic libraries at both UoN and CUEA had experienced challenges is responding to digital content disasters attacks based on factors such as; Lack of policies, unreliable internet attacks protection and unskilled manpower. Cybercrime has posed to the great extent on the smooth running of the two university libraries, respondents agreed that library databases of the universities were vulnerable to attacks launched by detractors, through hacking, spreading of worms or viruses. Information in the university libraries was not well preserved making websites to disappear frequently and digital media becoming obsolete easily. The university libraries did not have the prerequisite security mechanisms appropriate for internet based, applications in all its digital setups and maintenance. The two universities did not have an all-inclusive committee charged with the task of mitigating any disaster that may affect the institutions (78.6%), making the library very vulnerable to attacks. The University management also lacked adequate security measures to respond to cybercrime at the shortest time possible. In any institution securing digital content information system is coming up with controls and mechanisms to reduce or clear digital content threats to network security (Fitzgerald and Dennis, 2002).

The findings of this study imply that there is clearly inadequate disaster preparedness at the two Universities libraries with regards to digital content vulnerability. It is in agreement with Hlabaangani and Mnjama (2008) which asserts that majority of information centers, academic libraries included in many institutions lack disaster preparedness plans having inadequate policies and procedures, lack of trained staff on disaster preparedness and management. It is also revealed that there is inadequacy in the existing disaster preparedness plans where the respondents indicated that though there are disaster plans put in place at the universities, they are not specific to digital information resources preservation.

Recommendations

There is need to have the university library management to come up with specific digital content insecurity disaster preparedness policies and ensure their implementations to the letter. There is also need for library management to orient and train IT infrastructure library staff and other employees on the trends of cybercrime so as to adequately prepare them to timely respond to any digital content vulnerability attacks. The university should ensure continuous training staff and users on library security to ensure that they are updated with current knowledge and skills relating to digital security and preparedness. It is also recommended that the two libraries under this study and any other institution of higher learning should consider increasing budgetary provisions of adequate funds for training and retraining of staff and users in equal measures. The institution should have and enforce policies that guide on passwords, privileges, internal controls and have disaster recovery procedures as well as test-run them semi-annually at the minimum. University digital libraries should explore more methods of ensuring Security of digital contents in the areas of preservation and system backup to put in-check obsolescence of media storage issues.

References

Al-Suqri M. & Afzal W. (2007). Digital age: Challenges for libraries. *Information, Society and Justice*. *1*(1), 43-48. doi: 10.3734/isj.2007.1105.

Goodluck Ifijeh, Jerome Idiegbeyan-Ose, Chidi D Isiakpona, Julie Ilogho (2018). Library Science and Administration: Concepts, Methodologies, Tools, and

Jain, P. & Bentley, G. (2008). Institutional repositories as a benchmark for digital scholarship.

Khan, M. A. (2013). IPR in India and USA: Its impact on library services.

Kuzma, J. (2010). European digital libraries: Web security vulnerabilities. *Library Hi Tech*, *28*(3), 402- 413. doi: 10.1108/07378831011076657.

Lampson, B. (2004). Computers security in the real world. *Computer, 37*(6), 37-46.

Makori, E. O. (2009). Reinventing Academic Libraries in Kenya. *Library Hi Tech News*, No. 5-6: 10-13.

Moahi, K. H. (2009). Institutional repositories: Towards harnessing knowledge for African development. First International Conference on African Digital Libraries and Archives (ICADLA1).

Neuhaus, P. (2003). Privacy and confidentiality in digital reference. *Reference & User Services Quarterly*. *32*(1).

Njoroge (2014). An investigation on disaster preparedness and mitigation forcomputer based information systems in selected university libraries in Kenya.

Patel, A., Qassim, O. and Wills, C. (2010). A survey of intrusion detection and prevention systems. *Information Management & Computer Security, 18*(4), 277-290.

Vermaaten S, (2012): Identifying Threats to Successful Digital Preservation: the SPOT Model for Risk Assessment, doi: 10.1045/september2012-vermaaten

Zimerman, M. (2010). Protect your library's computers. *New Library World, 111*(5/6), 203-212. doi: 10.1108/03074801011044070.