Afr. J. Lib. Arch. & Inf. Sc. Vol. 33, No. 1 (April 2023) 1-21

Fostering Cybersecurity in Institutional Repositories: A Case of Nigerian Universities

Ifeoma Stella Njoku
The Library,Federal University of Technology,
P.M.B. 1526 Owerri, Nigeria.
somanjoku@gmail.com,
ifeoma.njoku@futo.edu.ng

Buniechukwu Chidike Njoku
Department of Science and Technology,
University of Burgundy France.
buniechukwunjoku@etu.u-bourgogne.fr,
bunienjoku@gmail.com

Scholastica A. J. Chukwu
The Library, Federal University of Technology,
P.M.B. 1526 Owerri, Nigeria
nnechika2005@gmail.com,
austinjanek2@yahoo.com

and

R. Ravichandran
Resource Centre, National Institute of
Technical Teachers Training and Research
Taramani Chennai 600113, Tamil Nadu, India.
keelairavi@hotmail.com, ravi@nitttrc.ac.in

Abstract

Some Nigerian universities are digitising their scholarly heritage and the high risk of loss or attack of digital records due to viruses and cyber hacks is worrisome, with far reaching consequences on the confidentiality, integrity and availability triad. This paper examines cybersecurity and institutional repository (IR) protection in Nigeria, highlighting the impact of cybersecurity and risk management. The study explores the five core frameworks of cybersecurity with emphasis on strategies for policy development and management of risk. It also analyses security threats through feedback from professionals in the referenced domain. A manual assessment was conducted with all Nigeria institutional repositories registered on opendoar.org using qualitative descriptive analysis. The sample size of the study consists of 88 librarians and information, communication and technology workers. A structured questionnaire on threats and risks of institutional repositories in Nigeria were distributed and 62(70.4%) responded. Results show that, of 198 federal, state and private universities, only 29 (14.6%) have established institutional repositories with slow adoption rate of 12.5% from 2009 to 2020, and 2019 having the highest established IR at a growth rate of 24%. Total number of items uploaded was 22,828. This paper found that DSpace open repository software had 79.3% use among institutions, while 26 institutions (89.6%) have uploaded journal articles. Hardware and software threats stood out prominently as leading causes of sub-optimal repository performance. Evaluated against an assigned weighted point system (of 31) derived from number of technical workers in IR domain, data reveals malware and malicious code as the biggest risk to repository resources, with 30.6%, followed by password attacks at 28% and IP theft 27.8% points respectively. However, hardening security systems guarding institutional hardware, software and infrastructure such as; management of identity access and operation, secure network application and data, could reduce incidents of cyber-crime. The research study recommends the development of modern cybersecurity framework for university libraries, mechanism for data defenses and redundancy strategies such as decentralisation of data and networks to mitigate the risk of vulnerability to attack and reduce loss from cyber incidents.

Keywords: Cybersecurity, Cybercrime, Cyber Attack, Institutional Repositories, Open Research, Digital Resources.

Introduction

The development of information technology (IT) and networked systems in the world has positive attributes on the institutional repositories. This migration of conventional repository to digitised format available on software, hardware and internetworked infrastructure has put host and delivery systems at great risk from threats like denial of service, malware, adware, ransom ware, virus attacks, social engineering, illegal data access, data theft, data confidentiality attacks and compromise of data integrity.

The concept of cybersecurity has been prompted by the need to provide seamless protection of data and information. Cybersecurity is the body of plan, policies, guidelines, approaches, actions, training, practices, assurance and technologies that can be used to protect the organisational assets such as computing devices, personnel, infrastructure, applications, services, telecommunications systems, and all the transmitted and stored information in the cyber environment (*International Telecommunication Union, 2012*). The rapid evolution of cyber attacks has led to concepts such as; Cybercrime as a service, encompassing concepts such as Malware-as-a-service and Phising-as-a-service. These concepts offer end-to-end services for malware distribution and spam attacks in digital environment. Cybercrime is on the increase and the cost has a cumulative effect on victims and organisations involved in cyberspace losses. Cybercrime undermines the overarching benefits of IT in achieving a scholarly environment. Incidents in 2011 affected over 40 million people in the US, 54 million in Turkey, 20 million in Korea, 16 million in Germany, and more than 20 million in China (McAfee, Intel Security, 2014).

Cyber-attacks incur an annual cost to the global economy of more than $400 billion in losses, which is more than national income of some countries (Lewis and Baker, 2013). Forbes (2015) asserts that the global cybersecurity market capitalisation as at 2015 was $75 billion and is expected to hit $170 billion in 2020. However, most countries and organisations underestimate the risk they face from cybercrime and how quickly this risk can grow. Evidence shows that Internet protocol theft and recovery loss accounts for the cost of cybercrime and its impact on national income that would otherwise be used for national development.

A study by Intel system on 51 countries in all regions of the world which accounts for 80% of global income shows that there are variations of losses among countries and Nigeria falls into a moderate confidence rating of 0.8% cybercrime tracking per gross domestic product (GDP) (McAfee, Intel Security, 2014).A 2022 Sophos Whitepaper concluded that 66% of organisations were affected by cyber attacks in data encrypted ransonware, with average ransom payments amounting to over $812,360 in the same period (Sophos, 2022). This data reveals that despite attempts by the state departments and agencies of security like National Information Technology Development Agency (NITDA) in Nigeria, there is still an overwhelming influence of threat actors on national and organisational integrity, resulting in financial loss (Madobi, 2023 and Ezeh, 2022).

A report by the National Communications Commission (2017) shows that about 91 million Nigerians use the Internet. This accounts for more than 48.9% of the population- one of the highest in Africa. Consequently, Nigeria ranks third with 5.8% among the top ten countries in the world with the highest individual perpetrators in cybercrime (Internet Crime Complaint CentreIC3 Report, 2010 and IC3 Report, 2017). Nigeria has been struggling with data theft issues, piracy and vandalism. Institutional repositories are not spared as they face the challenge of cybersecurity. The most common exploitation techniques of cyber crime in institutional repositories consist of social engineering, a situation where cybercriminals use programming or implementation failure to gain access to information (Anderson, Barton, Bohme, Clayton, Van Eeten, and Levi, 2012). A study of 600 students in tertiary institutions in Ekiti State, Nigeria to determine students' participation in cybercrime in Federal University of Oye-Ekiti, Ekiti State University and Afe-Babalola University shows that phishing, data theft and plagiarism are significant cybercrime in Nigeria (Omodunbi, Odiase, Olaniyan and Esan, 2016). According to finding by Adetoro and Okike (2020) on threats to the operating systems across the selected university libraries, malware was the major threat to the database/OPAC systems with a mean value of 62%, viruses and wormsa mean value of 60%, while, external hacking had a mean value of 31.7%.These effects diminish investment in research and also reduce the global rate of technological development.

An investment in research preservation, accessibility and visibility is to create innovation, attract users and competitors. Weak cyber law enforcement encourages cyber criminals and inhibits organisations and country's ability to build innovative infrastructure and development. Thus, the need for effective institutional repository protection achieved through institution, national and international policies and implementation, counter defence attack and preventive systems. Institutions are thereby required to influence and develop policy to enable Nigerian higher education realise the benefits of open research.

Nigeria has one hundred and ninety eight (198) federal, state and private universities (National Universities Commission, 2022). The study focuses on the protection of institutional repositories in Nigerian university libraries as they have in recent years, joined the open access to information in making scholarly publications available to the global community in the quest to link indigenous information heritage access to the world. Yet, inadequate data security, security framework policy and implementation continue to demean information protection. One of the recent challenges encountered by the library as it manages institutional repository is poor performance of the network firewall, which exposes the IR server to cyber-attacks (Chisita and Chiparausha, 2021). Some of the ways of reducing such menace includes; ensuring that institutions protect their information technology infrastructure such as computer systems and networks, computer architecture and details of configuration guideline.

Statement of the Problem

The Nigeria university libraries have in recent years, joined open access to information in making scholarly publications available to the global community in the quest to host indigenous (research) information heritage access to the world. However, inadequate data security framework, data loss management and physical implementation continue to degrade information protection. More challenges due to gaps in the protection of cyberspaces are weak digital intelligence, weak laws and implementation for cybercrime which means that domestic vendors face little risk of arrest and prosecution. The gap makes cyber criminals successful at the national level and even across borders. Nigeria needs to create strong laws to check data loss, promote data management and encourage the growth of institutional repositories. The study explores security threat analysis and risk, and recommend directives for cybersecurity implementation in university libraries to protect valuable repository data.

Objectives of the Study

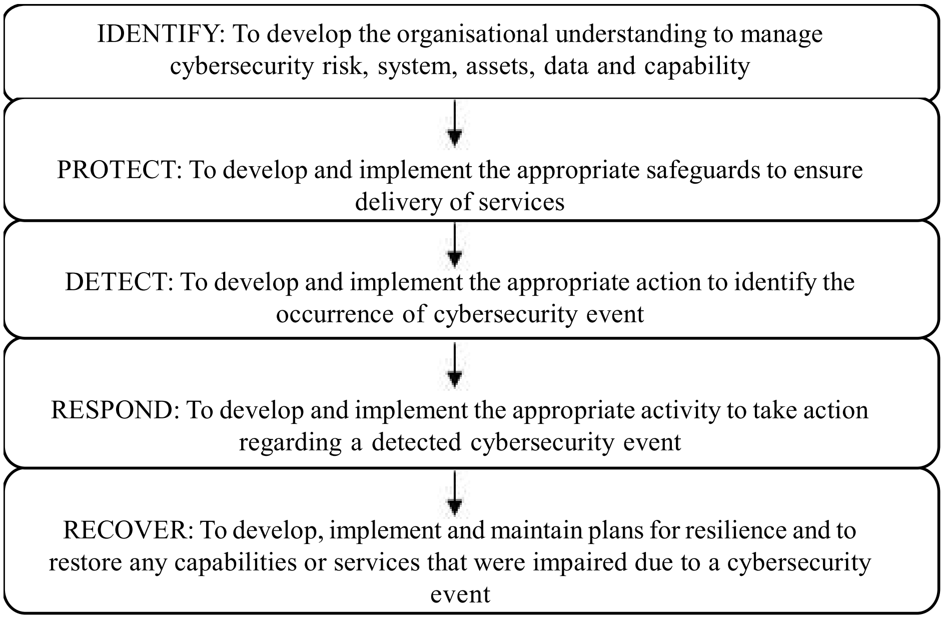
This work analyses the impact of cybresecurity threats on libraries and institutional repositories. The study focuses on the protection of institutional repositories of university libraries in Nigeria. This work aims to establish an inventory of threats to institutional repositories in Nigeria.

Research Questions

1. What are the university libraries that have established institutional repositories in Nigeria?
2. What are the software platform adopted for the institutional repositories in Nigeria?
3. What are the content types of resources in the institutional repositories in Nigeria?
4. What are the security threats to institutional repositories in Nigeria?

Cybersecurity Framework

Technological organisations are promoting policies and strategies to deal with the problem of cybersecurity. The National Institute of Standards and Technology (NIST) (2014) for example, established guideline in its framework that encourages checks and evaluation. See figure (1) below for the framework.



IDENTIFY: To develop the organisational understanding to manage cybersecurity risk, system, assets, data and capability

PROTECT: To develop and implement the appropriate safeguards to ensure delivery of services

DETECT: To develop and implement the appropriate action to identify the occurrence of cybersecurity event

RESPOND: To develop and implement the appropriate activity to take action regarding a detected cybersecurity event

RECOVER: To develop, implement and maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event

Figure 1: Framework of Cybersecurity

***Source*:** The National Institute of Standards and Technology (2014). Framework for improving critical infrastructure cybersecurity. *https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.1-with-markup1.pdf.*

This framework's five core functions are intended to perform concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk in the development, implementation, maintenance, and services of cyber networks. The framework focuses on cyber security context, function and risk that deals with organisational management strategy as a top priority. Implementation of the framework is based on the organisational determination for effective service delivery and maximisation of investment and outcomes. Though the framework was updated in 2017 to include feedback which makes it easier to use. The new framework did not replace existing management tools and policies in the model but identified gaps in the previous processes and developed models for improvement and management of the risk of cyber invasion. The most important response to cybercrime are policy and decision therefore, institutions are to manage the loss from cybercrime by deciding on the level of investment required to reduce the risk of cyberespionage and improve cyber supply chain risk management.

Institutional Repositories in Nigeria

Institutional repositories reflect the social-economic and indigenous knowledge value of a society. These collections represent the cultural heritage of a society consisting of data base of research output of an institution. Nath, Joshi and Kumar (2008) define it as a digital achieve of an institutions intellectual capital. Salawu (2010) asserts that it is an expression and communication of a community locally owned and adopted knowledge, as well as experience cumulated over the time for communication to the international community. This also showcase to the international community social economic cultural value of a communal knowledge. The need for institutional repositories according to Ridwan (2015) is to enhance open access research and scholarly output to national and international community. Ghosh and Das (2007) Ivwighreghweta (2012) maintain that institutional repositories encourage the free availability and dissemination of scholarly research globally. Mohammed (2013) states that institutional repository has become an information and communication technology channel through which academic research communities make their scholarly product visible to user. While, Nath, Joshi and Kumar (2008:52) assert that it is an open access gateway that preserves and disseminates the knowledge of institution through network with the aim to achieve institutional scholarly output that forms part of a larger global system of repositories using a standardised searchable interface (OAI-PMH). The release of OAI- PMH version 1.0 and version 2.0, open access repositories became more interoperable and this invention catalysed the progression of Institutional Repositories (Lagoze and Sompel, 2003). This development has opened up new ways of information harvesting, accessibility and dissemination of open knowledge globally thus, closed barriers of representation of cultural heritage of Nigeria.

Nigeria has one hundred and ninety eight (198) federal, state and private universities (National Universities Commission, 2022). Twenty nine or 14.6% universities have digitised some of their resources and uploaded to open access directory (*OpenDOAR, 2022).*Umar, Musa, and Aliyu (2014) write that some libraries in Nigeria have initiated the digitisation project into self-archiving open source software such as DSpace and Eprints.

Security Issues for Institutional Repositories

Though there are processes where traditional authentication and authorisation are required, access to digital environments requires security between a user's browser and a web server. There are scenarios of unauthorised users getting access to important websites and information theft through Internet Protocol authentication and password cracking. To evade these scenarios, access management control relates the remote identity information necessary to the service manager for authentication to enable an identification decision (Smith, 2002). Access identification login and password security are technologies that eliminate access vulnerability. Different authentication measure includes: Login identification, Sign-in and Password access (Antón, 2007). The primary use of a computer login procedure is to authenticate the identity of any computer user or computer software attempting to access the computers services (Stathopoulos, Kotzanikolaou and Magkos (2006).

Reasons for security control access to materials in a repository may include user authentication, digital material authentication, authorisation and identification. The foundation of safeguarding digital environment lies in dynamic change process strategy practices that require standards, collaboration and communities. Adequate security is expedient to secure system architecture and configuration information. This is to avert security threat emanating from traffic and use of network system. Security traffic analysis against threats consists of share, embed and analyse operations.

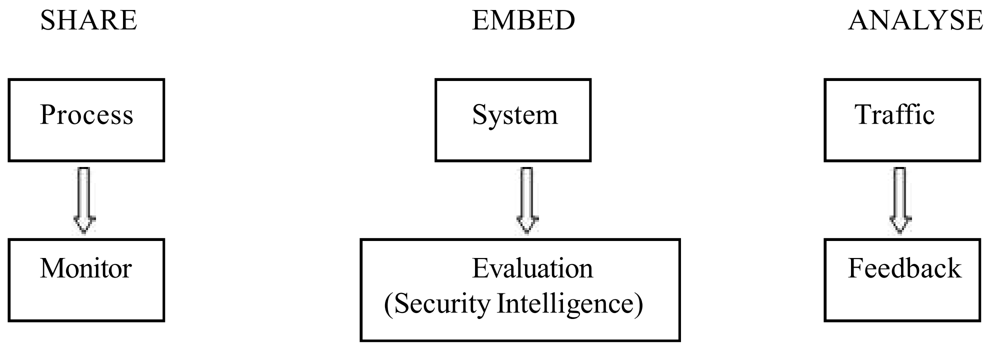


Figure 2: Security Traffic Analysis: ***Model by Authors: Njoku, I.S., Njoku, B.C., Chukwu, S.A.J. and Ravichandran, R.***

Effective monitoring, evaluation and feedback are used to develop confidentiality security authentication that safeguard digital platforms. Modeling and risk analysis consist of security intelligence and protection of critical systems and assets such as software, hardware and virtual private networks. Emphasis on protection of infrastructure like networks and computer systems is to avert damage indices and promote recoverability.

When developing an institutional repository, analysing and determining the digital identity and security of content is a major objective. Emphasis is on the type of technology, digital content, security of the systems / communication channel, diversity of users' platform and diversification responses at end users.

However, there are adverse negative effects presented through various attack vectors; the most prominent being malicious mail attachments, web page content, port scans, networked internet externally exposed ports. Also, attack surfaces such as databases, data entry, files, e-mail and other messages, cloud and local storage, login point are prone to malicious attacks.

Counter measures and protection mechanisms should be institutional goals to reduce the potential for threat and overall risk. Common measures are change control processes, physical entryway locks and barriers, passwords, firewalls and virtual private network tunnels. Vulnerability scan on data infrastructure in institutional repository can be performed with software as Nessus, Nexpose, Qualys, Nmap and web application scanners such as Skip fish, Arachni and IBM App.

Digital repository requires expertise in information technology, collection development, resource description, project management and high investment for maintenance of resources. These barriers account for the slow adoption of this initiative in developing nations. The United Nations (2010) resolution on cybersecurity encourages the creation of a global culture of cyber security and taking stock of national efforts to protect critical information infrastructures. One of the biggest challenges of cyber security is the quick rate at which in security risk[s] evolve. Discouraging cybercrime is the responsibility of a national cybersecurity and critical information infrastructure protection strategy that includes: the adoption of adequate legislation against the misuse of ICTs for criminal or activities intended to affect the integrity of national technological infrastructures. This responsibility requires coordinated action related to prevention, preparation, response and recovery from incidents and on the part of government institutions, private sector and citizens (International Telecommunication Union, 2012).

Cybercrime is a threat against various institutions connected to the Internet through their computers. Institution repositories strategies call for protection of data and information resources in the networked environment. In this regard, access management has emerged as major issue which hinders progress. While considerable work has been done in past decades within institutions and, more recently in support of digital repository, new policy issues emerge in the organisational access management control context. Weak security framework, poor implementation of infrastructure services, such as role-based access control; authorisation and authentication user and password protection are among the challenges facing institutional repositories. Without a proper access management method, confidentiality and integrity of information cannot be guaranteed. In most cases in-built mechanisms for security in repository software and operating systems are adopted for users' authentication, authorisation, digital rights and permission.

Methodology

Qualitative descriptive analysis was used for the study. Data collection shows that 29 out of 198 Nigeria federal, state and private universities have established institutional repository managed by Directory of Open Access Repositories (OpenDOAR, 2022).Manual assessment of institutional repositories establishment, use and security was conducted on 29 Nigerian Universities registered on Opendoar.org (2022). Data is presented with tables, frequencies, graphs, and result findings discussed. This study was conducted in March 2022. An update on the analysis was conducted in February 2023.

Table 1 below shows the Nigerian universities registered with OpenDoar. OpenDoar is a directory of open access institutional repositories. It is a quality-assured global directory that enables the identification and search for repositories to countries of the world (Opendoar.org. 2022).

Table 1: List of Nigerian Universities Registered with Opendoar

Nigerian Universities Registered with Opendoar					Metadata Count/ Subject	
S/N	**Universities**	**Content**	**URL**	**Software**	**Metadata**	**Subject Type**
1	ABU DSpace	Journal Articles	http://kubanni.abu.edu.ng/jspui	DSpace	8449	Multidisciplinary
2	Afe Babalola University Ado-Ekiti	Journal Articles	http://eprints.abuad.edu.ng/cgi/oai2	EPrints, Version: 3	744	Multidisciplinary
3	African Digital Health Library	Theses and Dissertations	http://adhlui.com.ui.edu.ng/	DSpace	1196	Health and Medicine
4	African Digital Health Library-University of Ibadan	Theses and Dissertations	http://adhlui.com.ui.edu.ng/	DSpace	1196	Health and Medicine
5	Ahmadu Bello University Zaria	Conferences; Workshop papers, Theses and Dissertations Journal Articles	http://www.abu.edu.ng/pages/researchworks	DSpace, Version: 5.5	7970	Science Agriculture, Food and Veterinary Arts and Humanities
6	Ambrose Alli University Ekpoma Institutional Repository	Journal Articles, Theses and Dissertations	http://154.68.224.61:8080	DSpace		Multidisciplinary
7	American University of Nigeria (AUN) Digital Repository	Journal Articles, Theses and Dissertations, Book Chapters and Sections, Other Special Item Types	http://digitallibrary.aun.edu.ng:8080/xmlui/	DSpace		Multidisciplinary
8	Covenant University Ota Electronic Theses and Dissertation Repository	Theses and Dissertations	http://eprints.covenantuniversity.edu.ng/	Institutional	10	Multidisciplinary
9	Covenant University Repository	Journal Articles	http://eprints.covenantuniversity.edu.ng/	EPrints, Version: 3.3.7	13259	Science Technology Social Sciences Law and Politics
10	dspace.funai.edu.ng	Journal Articles, Conference and Workshop Papers, Theses and Dissertations	http://dspace.funai.edu.ng/	DSpace	256	Multidisciplinary
11	Ebonyi State University Abakaliki	Journal Articles, Theses and Dissertations	http://ir.ebsu.edu.ng:8080/	DSpace, Version: 1.7.0	814	Multidisciplinary
12	EUSpace	Journal Articles, Book Chapters and Sections	http://repository.elizadeuniversity.edu.ng	DSpace	1220	Arts and Humanities Science Social Sciences Technology

13	Federal University Dutsin-ma Institutional Repository	Journal Articles, Bibliographic References, Conference and Workshop Papers, Theses and Dissertations ,Book Chapters and Sections	http://dspace.fudutsinma.edu.ng/jspui/	DSpace,		Multidisciplinary
14	Federal University Lokoja	Journal Articles	http://repository.fulokoja.edu.ng/	DSpace, Version: 5.2	89	Science General Arts and Humanities Genera
15	Federal University Ndufu-Alike Ikwo	Journal Articles; Report and Working Papers	http://dspace.funai.edu.ng/	DSpace	256	Multidisciplinary
16	Federal University of Technology Minna	Journal Articles; Theses; Learning Objects	http://dspace.futminna.edu.ng/jspui/	DSpace, Version: 1.8.2	4454	Multidisciplinary
17	Federal University of Technology Akure	Journal Articles, Bibliographic References, Theses and Dissertations	http://dspace.futa.edu.ng:8080/jspui/	DSpace, Version: 1.7.2	2346	Multidisciplinary
18	Federal University Oye-Ekiti institutional repository	Journal Articles	http://repository.fuoye.edu.ng/	DSpace	1166	Multidisciplinary
19	Federal University Oye Ekiti Repository	Journal Articles, Reports and Working Papers, Learning Objects, Other Special Item Types	http://www.repository.fuoye.edu.ng/	DSpace	1166	Science and Technology, Agriculture, Social Sciences
20	Landmark University Omu Aran	Journal Articles	http://eprints.lmu.edu.ng/	EPrints, Version: 3.3.12	507	Multidisciplinary
21	Landmark University Repository	Journal Articles, Bibliographic References, Conference and Workshop Papers, Theses and Dissertations	http://eprints.lmu.edu.ng/	EPrints, Version: 3.3.12		Multidisciplinary
22	Open Resources University of Nigeria Nsukka	Journal Articles, Theses and Dissertations, Reports and Working Papers	http://unn.edu.ng/chart/repo	UNSPECIFIED	22828	Multidisciplinary
23	Theses and Dissertations Covenant University	Journal Articles Conference and Workshop Papers, Theses and Dissertations Learning Objects	http://theses.covenantuniversity.edu.ng/	DSpace	233	Science , Technology Social Sciences Business and Economic Law and Politics Psychology

24	UILSPACE	Journal Articles, Theses and Dissertations	https://uilspace.unilorin.edu.ng	DSpace	734	Multidisciplinary
25	University of Ibadan Repository	Journal Articles. Bibliographic References, Conference and Workshop Papers, Theses and Dissertations, Books, Chapters and Sections	http://ir.library.ui.edu.ng/	DSpace	5104	Multidisciplinary
26	University of Ilorin	Journal Articles, Theses and Dissertations	http://uilspace.unilorin.edu.ng:8080/jspui/	DSpace		Multidisciplinary
27	University of Jos	Bibliographic References, Conference and Workshop Papers, Learning Objects, Other Special Item Types	http://dspace.unijos.edu.ng/	DSpace, Version: 3.2	1837	Multidisciplinary
28	University of Lagos	Journal Articles, Conference and Workshop Papers, Theses and Dissertations, Learning Objects	http://repository.unilag.edu.ng:8080/xmlui/	DSpace, Version: 3.2	674	Multidisciplinary
29	University of Nigeria Nsukka	Journal Articles, Theses and Dissertations. Books, Chapters and Sections	http://repository.unn.edu.ng:8080/xmlui/	DSpace, Version: 6.0	8674	Arts and Humanities Medicine Agriculture, Food Physics and Astronomy Social Sciences Technology
Total					85182	

Table 1 shows that from (2009-2020) a total of 29 open access institutional repositories have been established in Nigeria with a total of 85,182 uploaded. The University of Nigeria, Nsukka has the highest upload of 22,828 items. There was no metadata count record from OpenDoar for four institutional repositories under study.

Results

This study analysed the establishment of institutional repositories in Nigeria with OpenDoar institutional repositories statistical record for Nigeria educational institutions based on content, software, metadata count, subject type and security threats.

Table 2: Year, Number and Adoption of Institutional Repositories in Nigeria from 2009-2020

YEAR	NO OF IR
2009	1
2010	1
2011	1
2012	1
2013	3
2014	4
2015	5
2016	3
2017	2
2019	7
2020	1
Total	**29**

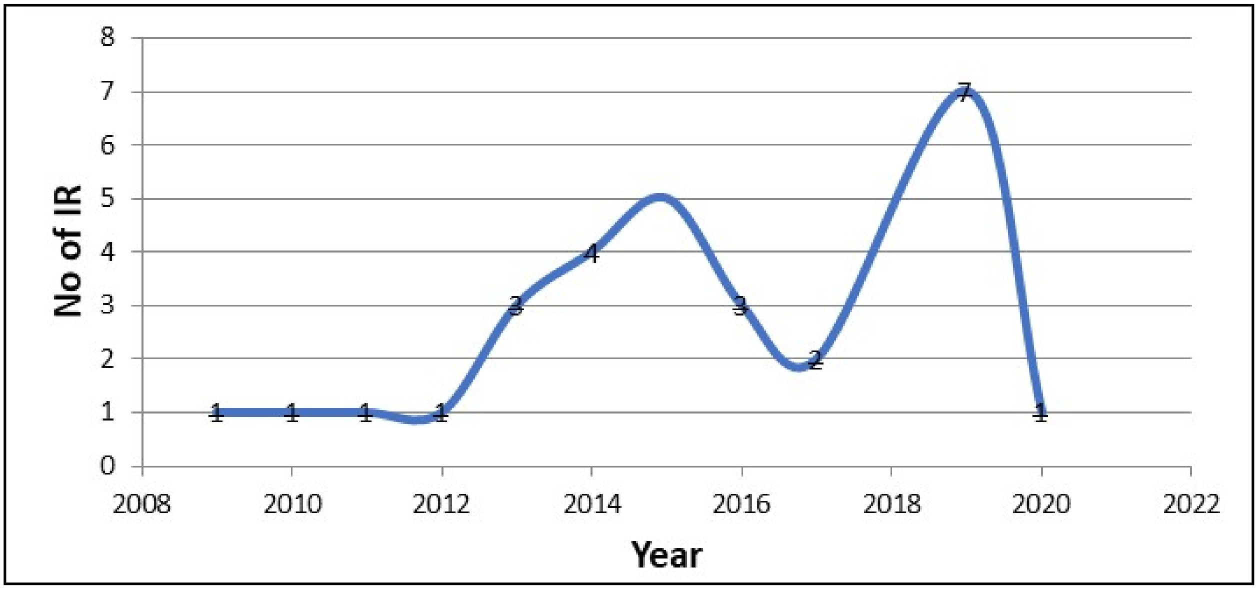


Figure 3: Year, Number and Growth of Institutional Repositories in Nigeria from 2009-2020

Data presented in Table 2 and figure 3 show the growth of institutional repositories in Nigeria from 2009-2020. The survey sample of 29 institutions show that 2019 had the greatest number (7) (24%), of institutional repositories, followed by 2015 which is (5) (17.2%) , 2014 were (4) (13.7%), 2016 and 2013 were (3) (10.3%), while 2017 had (2) (6.8%). Finally, 2009-2012 and 2020 were all (1) (3.4%). The table shows a slow growth rate of established institutional repository at 12.5% from 2009 to 2020 with its peak in 2019.

Table 3: Software Platform Overview

SOFTWARE	FREQUENCY OF USE
DSpace	23
Eprints	4
Institutional	1
Unspecified	1

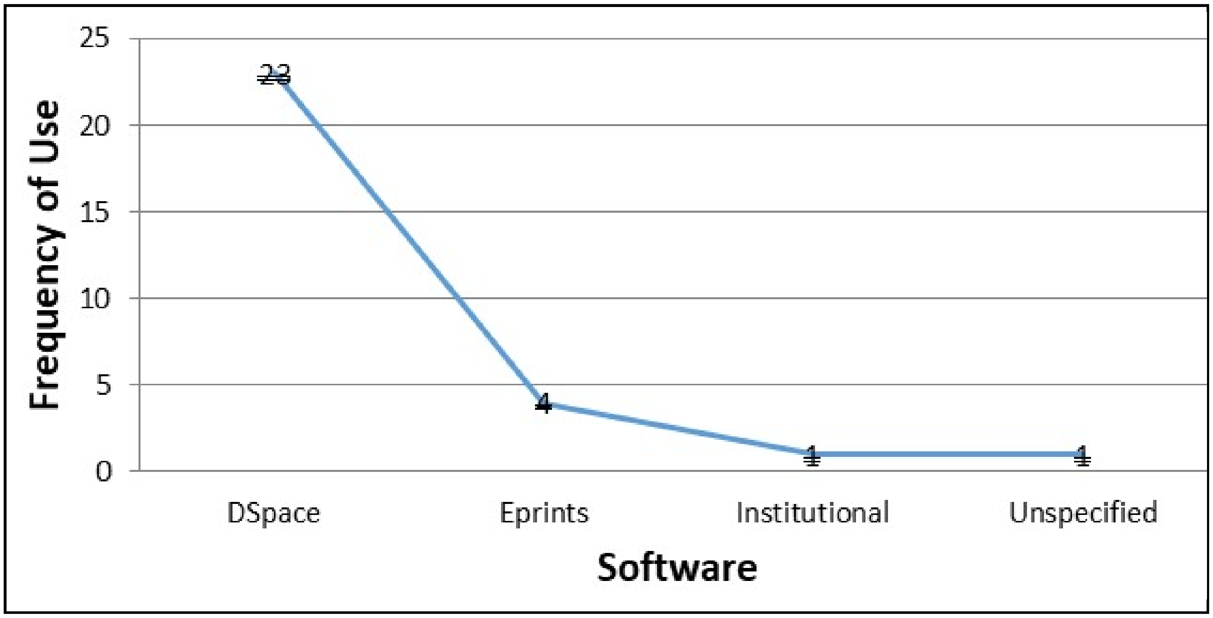


Figure 4: Frequency of Use of Software

Table 3 and figure 4: comprise of information on the software platform overview. The table shows that among the 29 institutions on the use of software, the majority indicated that (23) (79.3%) uses DSpace. Four used Eprint (4) (13.7%) and Institutional and Unspecified were (1) (3.4%) each.

Table 4: Content Types Overview

TYPES	NO OF UNIVERSITIES
Journal Articles	26
Theses and Dissertations	19
Book Chapters/Sections	4
Conferences and Workshop Papers	8
Report and Working Papers	4
Bibliographic References	4
Learning Objects	4
Other Special Item Types	4

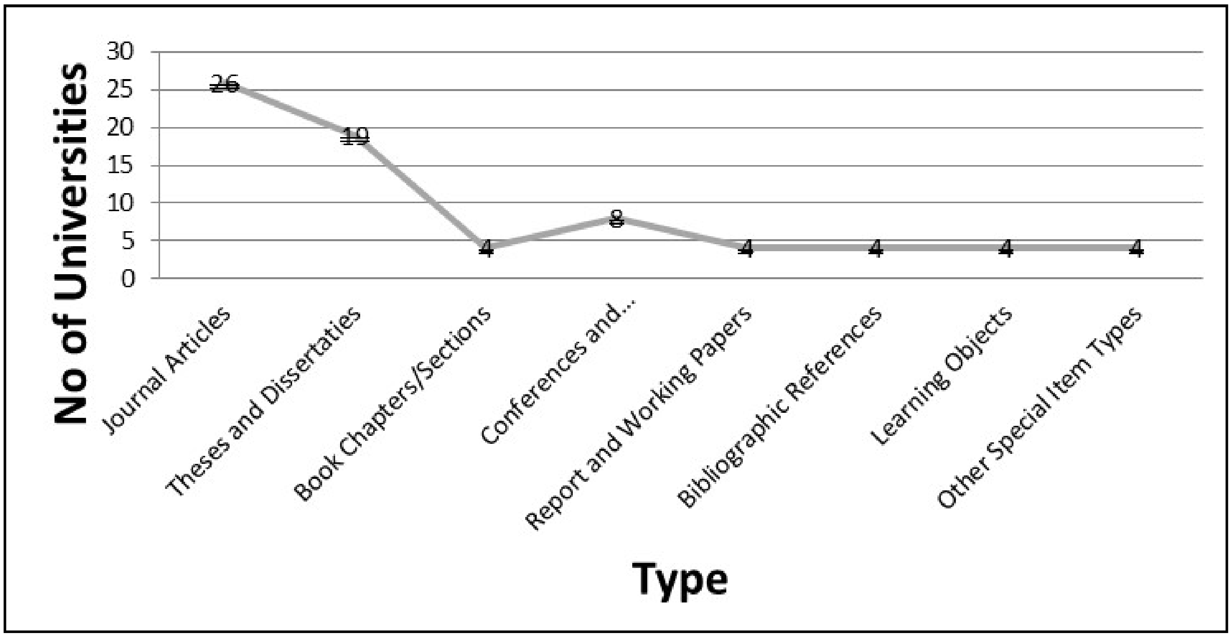


Figure 5: Content Types Overview

Presented on table 4 and figure 5 is information on the content types overview. The findings show that journal articles were the highest with (26) (89.6%), Theses and Dissertations had (19) (65.5%), Conferences and Workshop Papers (8) (27.5%), while others had (4) (13.7%) each.

Generaland Technical Survey: Cybersecurity Threats on Institutional Repositories in Nigerian Universities

Table 5
presents data from 29institutional repositories of Nigerian universities cybersecurity threats.

62 responses from librarians and information, communication and technology (ICT) staff, were classified into groups-

Physical: Referring to threats by human actors on system hardware. This class of attack includes breach of physical access control and damage of equipment and data.

Software: Referring to malicious pieces of computer code and programs designed to damage digital systems, and steal personal or financial information.

Infrastructure: Referring to threats to components of a network, including routers, firewalls, switches, servers that transport communications needed for service and content delivery.

Using a modified Likert scale, respondents offered insights on threats to library resources they had experienced while working. Responses were recorded to the question: Threat risk to the confidentiality, integrity and availability of institutional repositories.

Responses were also recorded for the indifferent option, for cases were the threat fell outside their domain of oversight.

Table 5: Security Threats on Institutional Repositories in Nigerian Universities

Question: Threat Risk to the Confidentiality, Integrity and Availability of Institutional Repositories.

General Survey- Cybersecurity Threats of Institutional Repositories in Nigerian Universities							Proportions				
Hardware Threats	**Strongly Agree (SA)**	**Agree (A)**	**Disagree (D)**	**Strongly Disagree (SD)**	**Indiffe-rent**		**Strongly Agree (SA)**	**Agree (A)**	**Disagree (D)**	**Strongly Disagree (SD)**	**Indiffe -rent**
Intrusion	35	24	2	0	1		56.45%	38.71 %	3.23%	0.00%	1.61%
Vandalism	34	14	6	2	6		54.8%	22.6%	9.7%	3.2%	9.7%
Theft	39	17	4	0	2		62.9%	27.4%	6.5%	0.0%	3.2%
Component Failure	34	18	6	4	0		54.8%	29.0%	9.7%	6.5%	0.0%
EMI (electro-magnetic interference)	10	16	5	5	26		16.1%	25.8%	8.1%	8.1%	41.9%
Software Threats	**Strongly Agree (SA)**	**Agree (A)**	**Dis-agree (D)**	**Strongly Disagree (SD)**	**Indiffe-rent**		**Strongly Agree (SA)**	**Agree (A)**	**Disagree (D)**	**Strongly Disagree (SD)**	**Indiff e-rent**
Malware/Malicious Code	24	33	2	3	0		38.7%	53.2%	3.2%	4.8%	0.0%
Ransomware	31	24	2	2	3		50.0%	38.7%	3.2%	3.2%	4.8%
Phishing	26	28	3	3	2		41.9%	45.2%	4.8%	4.8%	3.2%
Unauthorized Installation	38	24	0	0	0		61.3%	38.7%	0.0%	0.0%	0.0%
IP Theft	28	18	4	6	6		45.2%	29.0%	6.5%	9.7%	9.7%
SQL Infection	19	25	9	5	4		30.6%	40.3%	14.5%	8.1%	6.5%
Password Attacks	24	25	4	6	3		38.7%	40.3%	6.5%	9.7%	4.8%

Infrastructure Threats	Strongly Agree (SA)	Agree (A)	Dis-agree (D)	Strongly Disagree (SD)	Indifferent	Strongly Agree (SA)	Agree (A)	Disagree (D)	Strongly Disagree (SD)	Indiffe-rent
Packet Sniffing	21	16	10	6	9	33.9%	25.8%	16.1%	9.7%	14.5%
IP Spoofing	18	12	8	10	14	29.0%	19.4%	12.9%	16.1%	22.6%
DOS/DDos	14	16	16	8	8	22.6%	25.8%	25.8%	12.9%	12.9%
Session Hijacking	13	13	14	10	12	21.0%	21.0%	22.6%	16.1%	19.4%
Port Scans/Probes	14	17	16	4	11	22.6%	27.4%	25.8%	6.5%	17.7%
Total	422	340	111	74	107					
Average	24.82353	20	6.529412	4.352941	6.294118					
Proportion (%)	40.03795	32.25806	10.53131	7.020873	10.1518					

Analysing data from Table 5 hardware threats are widely regarded as the most important threats to service delivery in institutional repositories in Nigeria. Thirty-nine (62%) respondents strongly agreed that theft is the biggest threat facing repository resources due to insecurity in many regions of the country, followed closely by intrusion 35 (56%), vandalism and component failure 34 (54% each. Electromagnetic interference was the lowest with 10 (16%).

Analysing hardware threats, theft, intrusion, vandalism and component failure were the most commonly encountered threats to service delivery, while electromagnetic interference was the least common. Librarians and ICT workers believed that theft severely degrades repository performance. A further 27.4% of professionals in proportion (Table 5) corroborates this assertion in agreement that theft is a major cause for concern.

Software threats, majority of respondents acknowledged software threats as severe, with unauthorised installation 38 (61%) being the most probable software threat. Ransom ware 31(50%) IP theft 28 (45%) phishing 26 (41%) Malware and Password Attack 24 (38%) each, with SQL Infection being the least at 19 (30%).

Infrastructure threats produced the most even chart. A sizable number of respondents believed infrastructure threats are severe threats with Packet Sniffing 21(33%) and 25% agreed in proportional table 5.IP Sniffing 18 (29%), DOS and Port Scanning / Probes 14 (22%) each, and Session Hijacking 13 (20%).

On an interview checklist, a significant number of respondents 12 (19%) also stated that these threats fall outside of their technical domain.

It became evident that a sizable proportion of librarians believed that some cyber threats existed outside their domain of work. The electromagnetic interference {EMI} threat class particularly highlights this important variance in proportional Table 5 as Indifferent with 26 (41.9%). These librarians were unable to provide analytic feedback on security in this domain. Results from the software threats class also offer insight on a reasonable percentage of librarians in proportional Table 5 as indifferent with (IP Spoofing: 14 (22.6%), Session Hijacking: 12(19.4%), Port Scans/Probes: 11 (17.7%) who did not provide actionable information because they lacked technical oversight of these domains. As such, it became necessary to perform a more technical survey of cybersecurity issues according to data from 31 Information Communication and Technology technical workers and librarians involved in the infrastructure management, security management, security operations, disaster recovery and related roles. So another questionnaire was used to elicit information on core technical domain of institutional repository cyber security. See Table 6.

The Weighted Point Average is calculated as a mean value using the formula:

$\sum(\boldsymbol{Entries} * \boldsymbol{WP})/5$, where the number of individual responses recorded for any scale value (VLR, LR, MR, HR, VHR) assigned the value for "Entries". WP referred to the weighted point value (1, 2, 3, 4, 5) for any scale level. The product of Entries and WP (Weighted Points) was divided by 5, to derive a weighted point average for each threat class.

Table 6: Survey Technical Security Threats on Institutional Repositories in Nigerian Universities

Technical Survey – Cybersecurity Threats of Institutional Repositories in Nigerian Universities							
S/N	**Hardware Threats**	**Very High Risk-5**	**High Risk-4**	**Medium Risk-3**	**Low Risk-2**	**Very Low Risk-1**	**Weighted Points**
1	Intrusion	15	12	1	2	1	26.2
2	Vandalism	16	14	1	0	0	27.8
3	Theft	27	4	0	0	0	30.2
4	Component Failure	10	9	6	4	2	22.8
5	EMI	0	0	0	6	25	7.4
	Average						**22.8**
6	**Software Threats**	**Very High Risk- 5**	**High Risk-4**	**Medium Risk- 3**	**Low Risk- 2**	**Very Low Risk- 1**	**Weighted Points**
7	Malware/Malicious Code	29	2	0	0	0	30.6
8	Ransomware	1	1	1	13	15	10.6
9	Phishing	16	11	3	1	0	27
10	Unauthorized Installation	5	5	13	4	4	19.2
11	IP Theft	17	13	0	1	0	27.8
12	SQL Infection	0	0	4	3	24	8.4
13	Password Attacks	16	15	0	0	0	28
	Average						**21.65**
	Infrastructure Threats	**Very High Risk- 5**	**High Risk-4**	**Medium Risk- 3**	**Low Risk- 2**	**Very Low Risk- 1**	**Weighted Points**
14	Packet Sniffing	0	0	0	1	30	6.4
15	IP Spoofing	0	1	1	3	26	7.8
16	DoS/DDoS	2	5	3	20	1	16
17	Session Hijacking	1	1	1	15	13	11
18	Port Scans/Probes	1	0	2	2	26	8.2
	Average						**9.88**

Weighted point benchmark is 31

Table 6 presents the most important cybersecurity threats to institutional repositories. In reference to a weighted point benchmark of 31 points, the table above reveals that the highest threats to library repositories are hardware threats, with a weighted point average of 22.88, followed by software threats at 21.65 and finally infrastructure threats at 9.88.

The above result reinforces some of the findings in Table 5 given high value indifferent score. With this finding in technical survey, the study has been able achieve a better result by streamlining the data source. Evaluation of the technical survey revealed hardware threats to be quite prominent at 22.8 weighted average points, with most threats in this class being high risk or very high risk. Theft stood as the highest risk threat with 27 very high risk weighted points and 30.2 points on average. Theft is followed by vandalism at 27.8 average points, and intrusion at 26.2. EMI scored lowest with 7.4 points on average.

Considering software threats, Malware and Malicious code stood to pose the highest risk with 30.6 average weighted points, closely followed by Password Attacks, IP Theft and Phising. The least hazardous threats in this category were shown to be SQL Infection and Ransomware. Cummulatively, the software threats class has a mean weighted average of 21.65, right behind hardware threats in terms of severity.

Data shows that infrastructure threats at 9.88 mean-weighted points, held the lowest risk level against software and hardware threats. Most prominent threats in this category were rated as low risk or very low risk. The highest risk threat here was DOS/DDOS, followed by Session Hijacking. The lowest risk threats on the other hand are shown to be Packet Sniffing and IP Spoofing.

The weighted point is a 5-Point Likert Scale value (1, 2, 3, 4, 5**),** where Very High Risk (VHR-5), High Risk (HR-4), Medium Risk (VLR-3), Low Risk (VLR-2), Very Low Risk (VLR-1) and frequencies of occurrence.

Table 7: Cybersecurity Risk to Institutional Repositories Nigerian UniversitiesFrequencies of Occurrence.

Risk Rating	Risk Impact (Confidentiality, Availability, Integrity)	Frequency (Estimate)
Very High Risk (VHR-5)	Drastic, critical impact on service delivery and/or permanent asset loss	Once in 3 months
High Risk (HR-4)	Severe impact on service delivery and/or high technical and financial cost of asset recovery	Once in 6 months
Medium Risk (VLR-3)	Considerable impact on service delivery and/or difficulty with asset recovery	Once every year
Low Risk (VLR-2)	Minor impact on service delivery and/or quick asset recovery	Once every two years
Very Low Risk (VLR-1)	Negligible impact on service delivery and/or minimal asset loss	Once every 3 years

Table 7 shows that, drastic, critical impact on service delivery and/or permanent asset loss and severe impact on service delivery and/or high technical and financial cost of asset recovery occurred and once in three months and once in six months respectively. Hence a high need for universities in Nigeria to look inwards and support open research initiative achieved through institutional repositories and security of its hardware, software and infrastructure.

Discussion of Findings

Findings show that out of the 198 federal, state and private universities, only 29 representing 14.6% have established institutional repositories with slow growth rate of 12.5% from 2009 to 2020 at its peak in 2019. This collaborate the findings of Oguche (2018) that, Nigeria took nine years to register 23 repositories despite the number of higher institutions in Nigeria. Nene, Uzo and Baro (2021) assert that, universities in Nigeria are still struggling to overcome the many challenging issues. A study by Adam and Kaur (2021) buttresses the findings that implementation of institutional repositories has been very slow and the performance of the implemented repositories operates below expectation. This paper found that DSpace open repository software has 80% use among institutions. This confirms (Lynch, 2003) assertion that development of open access repository software, such as Dspace and Eprint also facilitated the development of institutional repositories. Adewole-Odeshi and Ezechukwu (2020) identify DSpace software as the preferred software for most of the repositories in Nigeria. Velmurugan (2013) maintains that the platform serves a variety of digital archiving needs. The finding also shows that journal articles has the highest content archived, this in line with Ukwuoma and Okafor (2017) finding that Covenant University and University of Nigeria Nsukka archived more journal articles. In addition, it justifies the assertion of Jamkar (2009) that the development of open access journals facilitated the establishment of institutional repositories in Nigeria. Analysing security, we were able to synchronise both security surveys. The general survey showed that a tiny percentage of respondents in Table 5 proportional value (6.5% -9.7%) disagreed that hardware threats were severe threats in all classes, while a sizeable number of professionals (42%) were unfamiliar with EMI threats. The technical study corroborates this by showing very high weighted points for all hardware threats except EMI. Furthermore, the general study put malware and malicious code as leading the software threat, in direct agreement with the technical study. Finally, the general survey revealed some bias against results of the technical one. The study also revealed packet sniffing and EMI to be the least severe threats.

Conclusion

Data security is the key to growth of Nigerian institutional repository content. The inability to secure an integrated database impedes investment in the innovative open access project. As more digital content of research output are deposited into institutional repositories, it is a huge concern for institutions and authors losing their published research to network hacking, cyber theft and virus attacks. Institutional repository security efforts should comprise of: management of identity, access and operations, secure networks, applications, data, and implement platform protection framework. Since the recovery process of cyber incident is expensive, security of data should be the utmost concern of institutions in preventing cyber-attacks with a view to growing Nigerian intellectual, scientific, cultural, scholarly heritage content sustainably.

Recommendations

The recommendations arising from this study are:

- ♦ Integration and compliance to a modern cybersecurity framework in libraries, addressing specific requirements of digital environments.
- ♦ Regulation review of the sector through development of standards, guidelines and policies to enhance cybersecurity resilience in Nigerian university libraries.
- ♦ Education and training of librarians on cybersecurity compliance in digital resource management.
- ♦ Sensitisation of users and the general public on benfits of adherence to established cybersecurity best practices.

- Development of mechanisms for redundancy and rapid response to mitigate data loss.
- Institutions special security operations monitoring centers to protect repositories.
- Decentralisation of data and networks.

References

Adam, U.A. and Kaur, K. (2021). Institutional Repositories in Africa: Regaining Direction. *Information Development*, 32(2).Available at; https://journals.sagepub.com/doi/abs/10.1177/02666669211015429(Accessed 25 February 2022).

Adetoro, Niran and Okike, B. (2020). Are there Threats to Information System Security: A Focus Nigerian University Libraries. *Gateway Information Journal 20 (1) 44-55.*

Adewole-Odeshi, E. and Ezechukwu, C. O. (2020). An Analytical Study of Open Access Institutional Repositories in Nigerian Universities. *Library Philosophy and Practice(e-journal)3884.* Available at: *https://digitalcommons.unl.edu/libphilprac/3884* (Accessed 25 February 2022).

Anderson, R., Barton, C. and Bohme R. Et al (2012). Measuring the Cost of Cybercrime (Paper Presented at the Weis 202 Workshop on the Economics of Information Security Berlin, Germany June 25-26, 2012). Available at: http://weis2012.econinfosee.org/papers/Aderson_WEIS2012.pdf.(Accessed 28 March 2017).

Anene, I. A., Uzor, S. E. and Baro, E. E. (2021). Institutional Repository Development in Nigerian Universities: Benefits and Challenges. *Niger Delta Journal of Library and Information Science* 1(1) Available at https://www.researchgate.net/profile/AneneIfeanyi/publication/344402672_Institutional_Repository. (Accessed 2 February 2022).

Antón, L., Jones A. and Earp, J.B. (2007). Towards Understanding User Perceptions of Authentication Technologies. Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society. Virginia: Association of Computer Machinery. Available at: https://www.researchgate.net/publication/228956678_Authentication_and_Authorization_Security_ Issues _ (Accessed 28 February 2002).

Chisita, C. T. and Chiparausha, B. (2021). An Institutional Repository in a Developing Country: Security and Ethical Encounters at the Bindura University of Science Education, Zimbabwe. *New Review of Academic Librarianship*, 27 (1) 130-143.

Ezeh, F. (2022). NITDA Raises Awareness over Cybersecurity. The Sun Newspaper Online 7th October 22. Available at: https://sunnewsonline. com/nitda-raises-awareness-over-cyber-security/ (Accessed 18 February 2022).

Forbes (2015). Cybersecurity Market Reaches $75 Billion in 2015. Available at: https://www.forbes.com/.../2015/.../cybersecurity-market-reaches-75billion-in-2015. (Accessed 28 March 2017).

Ghosh, S. and Das, A. (2007). Open Access and Institutional Repositories - A Developing Country Perspective: A Case of India. *IFLA Journal, 33:229-250.*

International Telecommunication Union (2012). Understanding Cybercrime: Phenomena, Challenges and Legal Responses. Available at :www.itu.int/ITUD/cyb/cybersecurit/legislation.html. (Accessed 29 November 2017).

Internet Crime Complaint Center (IC3) (2010). Annual Reports. Available at: www.ic3. gov>media>annuals reports. (Accessed 28 May 2017).

Internet Crime Complaint Center (IC3) (2017). Annual Reports. Available at: www.ic3. gov>media>annualsreports. (Accessed 11 November 2017).

Ivwighreghweta, O. (2012). An Investigation to the Challenges of Institutional Repositories Development in Six Academic Institutions in Nigeria. *International Journal of Digital*

Library Services, 2(2):1-16. Available at: *http://www.ijodls.in/uploads/3/6/0/3/3603729/vol-2_issue-4_1-16.pdf.*(Accessed 17 November 2019).

Jamkar, S. (2009). Library and Information Services in Changing Era. Conference at Jayakar Library, SPPU, Pune https Available at: *https://www.researchgate.net/publication/312551821_Institutional_ Repository*. (Accessed 17 November 2019).

Lagoze, C.and Van de Sompel, H. (2003). The Making of the Open Archives Initiative: Protocol for Metadata Harvesting. *Library Hi Tech 21(2)m118-128.*

Lewis, J. A. and Baker, S. (2013). Estimating the Cost of Cybercrime Center for Strategy and International Studies, Washington, D.C., June. Available at: https://csis.org/event/estimating-cost-cyber-crime-andcyberespionage. (Accessed 17 November 2019).

Lynch, C. (2003). Institutional Repositories: Essential Infrastructure for Scholarship in Digital Age Portal. *Libraries And The Academy 3* (2) 327-336.

Madobi, M. Y. (2023). NITDA Bill and Entrenchment of Cybersecurity. Guardian Nigeria Newspaper 3rd January 2023. Available at:*https://guardian.ng/technology/nitda-bill-and-entrenchment-of-cybersecurity/* (Accessed 18 February 2023).

McAfee Intel Security (2014). Net Losses: Estimating the Global Cost of Cybercrime. Available at: http://www.mcafee.com-reports-rp-e. (Accessed 18 August 2018).

Mohammed, A. (2013). Institutional Digital Repository: An Option for Scholarly Communication in Nigeria. *International Journal of Education and Research*, 1(6):1-10. Available at: *https://ijern.com/journal/June-2013/33.pdf.*(Accessed 17 November 2019).

Nath, S., Joshi, C. and Kumar, P. (2008). Intellectual Property Rights: Issues for Creating Institutional Repositories. *DESIDOC Journal of Library and Information Science,* 28(5):49-55.

National Institute of Standards and Technology (NIST) (2017). United States Department of Commerce Draft Version 1.1. Available at: *https://www.nist.gov/sites/default/files/documents////draftcybersecurity framewor kv1.1wi* (Accessed 28 August 2017).

National University Commission (2022). List of Accredited Universities in Nigeria. Available at: *https://www.nuc.edu.ng/nigerian-univerisities/private-univeristies/.* (Accessed 6 March 2023).

Nigerian Communications Commission (NCC) (2017). Stakeholders Information Statistics and Reports Industry Statistics. Available at: *www.ncc.gov.ng.statistics-reports.*(Accessed 28 August 2017).

Oguche, D. (2018). The State of Institutional Repositories and Scholarly Communication in Nigeria. *Global Knowledge, Memory and Communication*, (67) 1/2, 19-33.

Omodunbi, B., Odiase P. and Olaniyan, O. (2016). Cybercrimes in Nigeria: Analysis, Detection and Prevention. *FUOYE Journal of Engineering and Technology,* 1(1) 37-42.

OpenDOAR (2022). Open Access Countries and Organisations-Africa. Available at: *www.opendoar.org/countrylist.php.* (Accessed 26 August 2022).

Ridwan, S. M. (2015). Institutional Repository: A Road Map to Open Access and Resources Sharing in Nigeria Issues and Challenges. *International Journal of Scientific Engineering Research* 6(1) 598-605.

Salawu, B. A. (2010). Issues and Challenges in the Creation of Institutional Repositories with Local Content: Critical Reflections. *Journal of Information Society and Justice,*3(1) 59-68.

Smith, R. E. (2002). Authentication: From Passwords to Public Keys. Boston MA: Addison-Wesley Longman Publisher.

Sophos (2022). Ransomware Hit 66% of 2022 Organisations Surveyed for Sophos Annual State of Ransomware2022. Available at*: https://www.sophos.com › press-releases › 2022/04 › r.* (Accessed 18 February 2023).

Stathopoulos, V., Kotzanikolaou, P. and Magkos, E. (2006). A Framework for Secure and Verifiable Logging in Public Communication Networks. In: Lopez J. (eds) Critical Information Infrastructures Security. CRITIS 2006. *Lecture Notes in Computer Science*, 1(4347). Heidelberg, Berlin: Springer. Available at: *https://link.springer.com/chapter/10.1007/11962977_22#citeas*.(Accessed 28 August 2017).

Ukwuoma, S.C. and Okafor, V.N. (2017). Institutional Repository in Nigerian Universities: Trends and Development. *Library Collection Acquisition and Technical Services*, 40 (1-2) 46-57.

Umar, M. A., Musa, S. and Aliyu, A. (2014). Institutional Repositories in Nigeria: Issues and Challenges, *IOSR Journal of Humanities and Social Sciences* 19 (1) 16-21.

United Nations (2010). Cybersecurity Resolution: Global Security Agenda. Available at: *www.itu.int›action›cybersecurity›Pages›un-resolutions*. (Accessed 28 August 2017).\

Velmurugan, C. (2013). Open-Source Software: An Institutional Digital Repository System with Special Reference to Dspace Software in Digital Libraries-An Introduction. *Review Paper, International Journal of Library and Information Science*. 313-318. Available at: *http://www.academicjournals.org/IJLIS*. (Accessed 26 February 2022).

Ifeoma S. Njoku is a Senior Librarian and the Coordinator, Research Training and Statistics Unit of the Library, Federal University of Technology Owerri, Imo State, Nigeria. She is a Certified Librarian of Nigeria and has a PhD in Library and Information Science of Abia State University, Uturu.

Buniechukwu Chidike Njoku is an Integration Engineer with a Master degree in Advanced Electronic Systems Engineering program from Université de Bourgogne, France. He holds a Bachelor of Engineering degree in Electrical and Electronics Engineering (Communication Engineering) from the Federal University of Technology Owerri, Nigeria. He holds professional certifications including: Juniper Automation and DevOps Associate- 2020, Google Cloud Associate Cloud Engineer- 2020, Nokia Routing Specialist 1- 2019, Cisco CCNA CyberOps (Cybersecurity Operations) - 2018.

Scholastica A.J Chukwu is a Senior Librarian and a staff of the Federal University of Technology Owerri, Imo State, Nigeria. A Certified Librarian of Nigeria.

R. Ravichandran works at the Resource Centre National Institute of Technical Teachers Training and Research, Taramani Chennai, Tamil Nadu, India. He has experience of 34 years and has educational qualifications of four master's degree and Ph.D.