

Implementation of Network and Server Security Measures in Nigeria University Libraries

¹Yusuf Ahmed, ²Ibrahim Salihu Yusuf, ³Ahmad Aliyu and ⁴Ibrahim, Hauwa

^{1,2,3,4} Kashim Ibrahim Library, Ahmadu Bello University, Zaria. Nigeria

ahmedyusufkil@gmail.com ibrahimsalihuyusuf@yahoo.com aliyuahmad1434@gmail.com

Abstract

This study investigates the level of implementation of network and server security measures in federal university libraries to achieve two research objectives. Quantitative research methodology was adopted, and a survey design was used to explore the study population. 20 internet librarians were randomly selected across federal university libraries in Nigeria. The questionnaire was used as the instrument for data collection, and the data collected were descriptively analyzed using SPSS version 23 to calculate the mean and standard deviation, which form the basis for discussion. The study revealed the use of antivirus software, installing firewalls in the systems, installing wireless security products, limiting connection time, separating cables to differentiate public and staff's local area networks. The study also found out that placing the server in a secure location, Installation of antivirus software on servers, regular backups for the data, and Installation of intrusion detection software and host auditing software as the main server security measures implemented in Nigeria federal university libraries. Despite the availability of information security measures in the 21st century, librarians in Nigeria's university libraries have not fully implemented network and server security measures in protecting the library system. The study recommends that the library management should ensure full implementation of server segregation, the network is segmented with a router, and the installation of a firewall with virtual private network remote and wireless access to protect the university library network. Also, Systems Authentication, Restriction of the file system in a server, installation of firewalls, Review Server logs periodically, Hardening the library servers' operating systems (OS) and applications, and Implementation of fault tolerance should be adequately implemented by system administrators in the studied libraries to protect servers.

Keywords: Network Security, Server Security, Information Security, Security Measures, University Libraries

Introduction

The adoption of information technologies in libraries and information centers has created avenues for digitization of information content. This development necessitated the adoption of information security strategies to protect our digital assets and systems. Protecting digital assets will facilitate effective and efficient service delivery. To achieve this, libraries need to deploy a variety of information security management systems for ensuring digital asset safety (Mittal, Gupta, Chaturvedi, Shailesh, Chansarkar, & Gupta, 2021; Kim, 2020; Meth, 2019; Mustafa

&Kar, 2019). Ideally, information security processes prevent information systems from potential threats.

According to Kessler, Pindek, Kleinman, Andel, & Spector (2020), Information security threats affect the quality of service delivery in libraries and information systems. Discussions on security issues related to libraries enable us to identify and implement appropriate countermeasures. Libraries, where routine tasks are performed using current technologies, must be sensitive in assessing their information management processes. Threats prevention and information security countermeasures represent the major concern of the 21st-century libraries and information systems. As a result, Ngwum, Raina, Aguon, Taylor, & Kaza (2020) posit that libraries find it difficult to implement appropriate information security measures, especially in the area of their network and servers.

To understand information security measures implemented in Nigerian federal university libraries, scholars have investigated the problem from different perspectives, hardware, software, and workstation security (Ozkan, Yigit, Spruit, Wondolleck, & Verónica, 2020), data security (Padilla, 2019) and physical security. Despite these studies, the problem persists in federal university libraries, especially in the Nigerian context. Scholar (Velte & Wikle, 2020; Velte & Wikle, 2020; Wendzel, Levy-Bencheton & Caviglione, 2020) have stressed the need to view the problem from different perspectives (i.e., network and server security). To reduce the problem to the barest minimum, this study aimed at viewing the problem from a different perspective (i.e., network and server security).

Problem Statement

Preliminary investigation by the researchers revealed that federal university libraries in Nigeria are constantly experiencing network and server attacks which translate into a reputation and financial cost. Server crash in University Jos, ABU Zaria, and University of Nigeria SUKKA libraries has led to data loss which translates into financial loss if carefully analyzed. This loss is hardly discussed by the affected libraries even when their digital assets are at risk. The most dangerous information security attacks are targeted towards the library's network and servers. Despite these issues, federal university libraries in Nigeria hardly take security measures into consideration. This prompted the researchers to investigate issues related to the level of implementing network and server security in the universities under study.

Objectives of the Study

- a. To identify the level of implementation of network security measures in Federal University Libraries, Nigeria.
- b. To find out the level of implementation of server security measures in Federal University Libraries, Nigeria.

Literature review

San Nicolas-Rocca, & Burkhard (2019) conducted a study on the assessment of information security in Auckland public libraries. The study sought to achieve three objectives

which are: what are the software security threats in Auckland public libraries? What are the hardware security threats in Auckland public libraries? What are the workstation security threats in Auckland public libraries? The study adopted quantitative research methodology. A case study research design was used. 15 librarians were randomly selected as the study participants. The study revealed LAN cable vandalization and theft as the major hardware security threats in the libraries under study. Viral attacks and third-party intrusion were the software security threats. The study concluded that library computers are under siege, and libraries must take action to avert such problems. The researcher also recommends that public library authorities should encourage staff training on information security to secure the information systems.

Singh (2019) investigated information security in Academic libraries. Using descriptive research design, the study revealed that academic libraries experience data loss, hacking, and phishing attacks. The study further views quality librarianship as a lasting solution to the revealed information security challenges. The study recommends integration and installation of firewall, use of passwords, and system authentication as a way forward.

Yusuf, Sunusi, Omah & Suleiman (2021) investigated the implementation of hardware, software and workstation information security measures in federal university libraries of Nigeria. Descriptive survey was adopted as the research design. Four hundred and sixteen (416) Librarians were randomly sampled across federal university libraries in Nigeria to represent the population of this study. Questionnaire was used as the instrument for the data collection, and benchmark for analysis is determined as positive when the mean is 2.50 and above, while a mean of less than 2.50 is regarded as negative. The study revealed that the use of security cables to improve the safety of hardware devices, the use of CCTV in public IT areas and server areas had been found to be a physical security measure implemented in university libraries. The findings are also revealed that the use of timer software, cleaning software, web filtering software, library system, menu replacement software represent the software security measure implemented in university libraries. The study recommended that: The library management should ensure full implementation of locks and remote mirroring to backup all files in the system. System administrators should ensure proper implementation of user entrance lock to record and monitor user's security programs and desktop security programs. Rollback security implementation should be implemented to keep track to record of changes made to the system. The library management should ensure full implementation of firewalls as workstation security program. None of the reviewed studies investigates information security from a network and server perspective, especially in federal university libraries of Nigeria. This justifies the need for this research.

Methodology

Descriptive survey was adopted for this study. The method is found appropriate because it is more ideal for studying a spread population, and the population of librarians is spread across Nigeria. Twenty Internet Librarians were randomly selected across federal university libraries in Nigeria to represent the population of this study. Questionnaire was used as the instrument for the data collection. Mean, and standard deviation was used to analyze the data collected from the

respondents. The benchmark for analysis is determined as positive when the mean is 2.50 and above, while a mean of less than 2.50 is regarded as negative.

Findings and Discussion

Table1: Level of Implementation of Network Security Measures in Federal University Libraries in Nigeria

Network Security Measures	N	Mean	Std. Deviation	Remarks
The use of Antivirus software	20	2.85	1.27	Agreed
Installing Firewall in the systems	20	3.20	1.16	Agreed
Server segregation	20	2.30	1.31	Disagreed
network is segmented with a router	20	2.30	1.13	Disagreed
Installing Wireless security products	20	2.80	1.11	Agreed
Limiting connection time	20	2.80	1.28	Agreed
Separating cables to differentiate Public and staff's local area networks	20	2.85	1.18	Agreed
Installation of Firewall with virtual private network remote and wireless access	20	2.10	1.02	Disagreed

Table1 revealed the network security measures implemented in federal university libraries of Nigeria. The table shows that Installing a firewall in the systems with a mean value of 3.20 is the major network security measure implemented in the federal university libraries. It is also revealed that the use of antivirus software and Separating cables to differentiate Public and staff's local area networks (mean=2.85) are implemented in securing the networks of federal university libraries of Nigeria. Installing Wireless security products and Limiting connection time with a mean value of 2.80 each are found to be other network security measures implemented in federal university libraries of Nigeria. On the other hand, the respondents show some level of disagreement with the level of implementation of network segregation and segmentation with the router with a mean value of 2.30 each. The study participants also indicate a level of disagreement with installing a firewall with virtual private network remote and wireless access (mean=2.10) as a network security measure implemented in federal university libraries of Nigeria.

The study revealed that the use of antivirus software, installing firewalls in the systems, installing wireless security products, limiting connection time, separating cables to differentiate public and staff's local area networks as the major network security measures implemented in federal university libraries of Nigeria. Adoption of these measures to protect the library's network has to a great extent help the smooth operation of digital operation in the library's studies. The 21st century university library users solely depend on the efficient network to access

digital content of the library hence, the need for adopting appropriate measures to safeguard the network. This finding is in agreement with the discoveries of Ozkan, Yigit, Spruit, Wondolleck, & Verónica (2020), who asserts academic libraries of the 21st century have adopted different information security measures to prevent their internet connectivity.

Table 2: Level of Implementation of Server Security Measures in Federal University Libraries, Nigeria

Server Security Measures	N	Std.		Remarks
		Mean	Deviation	
Systems Authentication	20	1.95	0.70	Disagreed
Placing the server in a secure location	20	3.45	1.28	Agreed
Restriction of file system in a server	20	2.05	0.83	Disagreed
Installation of antivirus software on servers	20	3.50	0.83	Agreed
Installation of firewalls	20	2.05	0.69	Disagreed
Review Server logs periodically	20	1.90	0.85	Disagreed
Regular backups for the data	20	3.35	0.89	Agreed
Hardening the library servers' operating systems (OS) and applications	20	1.90	1.02	Disagreed
Implementation of fault tolerance	20	1.95	1.10	Disagreed
Installation of intrusion detection software and host auditing software	20	3.70	0.80	Agreed

Table2 revealed the server security measures implemented in federal university libraries of Nigeria. The respondents indicate that installation of intrusion detection software and host auditing software (mean=3.70) is the main server security measures implemented in federal university libraries of Nigeria. They also revealed the installation of antivirus software on servers with a mean value of 3.50 as another server security measure implemented in federal university libraries. Next is placing the server in a secure location (mean=3.45) as an implemented server security measure in the federal university libraries of Nigeria. The respondents also revealed that regular backups for the data (mean=3.35) is an implemented server security measure in the federal university libraries studied. The respondents also indicate that the federal university libraries studied did not implement Hardening the library servers' operating systems (OS) and applications(mean=1.90), Review of Server logs periodically (mean=1.90), fault tolerance (mean=1.95), Systems Authentication (1.95), Restriction of file system in a server (mean=2.05) and installation of firewalls (mean=2.05).

The study found out that placing the server in a secure location, installation of antivirus software on servers, regular backups for the data, and installation of intrusion detection software and host auditing software as the main server security measures implemented in Nigeria federal university libraries. This shows that the libraries have taken steps to address server security issues, but it is not enough because their other needed measures are yet to be implemented. If this is not addressed, then the heart of computing (servers) in the studied libraries will malfunction, and every digital activity in the system will be affected. The finding is in agreement with Yusuf, Sunusi, Omah & Suleiman (2021), who asserts that placing the server in a secure location, installation of antivirus software on servers, regular backups for the data and installation of intrusion detection software, and host auditing software represent the information security measures implemented in federal university libraries.

Conclusion

Despite the availability of information security measures in the 21st century, librarians in Nigeria's university libraries have not fully implemented network and server security measures in protecting the library system. These will expose the digital and virtual sections of the libraries to dangers such as crashes and data loss. Librarians need to exploit different security measures to prevent financial and reputation costs in the libraries.

Recommendations

1. The library management should ensure full implementation of server segregation, network is segmented with a router, and installation of a firewall with virtual private network remote and wireless access to protect the university library network.
2. Systems Authentication, Restriction of file system in a server, installation of firewalls, Review Server logs periodically, Hardening the library servers' operating systems (OS) and applications, and implementation of fault tolerance should be adequately implemented by system administrators in the studied libraries to protect servers.

References

- Kessler, S. R., Pindek, S., Kleinman, G., Andel, S. A., & Spector, P. E. (2020). Information security climate and the assessment of information security risk among healthcare employees. *Health Informatics Journal*, 26 (1), 461–473. 10.1177/1460458219832048 .
- Kim, B. (2020). Moving forward with digital disruption: What big data, IoT, synthetic biology, AI, blockchain, and platform businesses mean to libraries. *Library Technology Reports*, 56 (2), 1–32 .
- Meth, M. (2019). Barriers and challenges to blockchain implementation in libraries. *Library Technology Reports*, 55 (8), 20.
- Mittal, A., Gupta, M. P., Chaturvedi, M., Shailesh, R., Chansarkar, & Gupta, S. (2021). *Cybersecurity Journal of Intellectual Capital*, 21 (2), 235–256. 10.1108/JIC-05-2019-0128 .Enhancement through Blockchain Training (CEBIT)–A serious game

- approach. *International Journal of Information Management Data Insights* , Article 100001. 10.1016/j.jjime.2020.100001 .
- Mustafa, S. Z. ,& Kar, A. K. (2019). Prioritization of multi-dimensional risk for digital services using the generalized analytic network process. *Digital Policy, Regulation and Governance* Mar 8 .
- Ngwum, N. , Raina, S. , Aguon, S. , Taylor, B. , & Kaza, S. (2020). A model for security evaluation of digital libraries: A case study on a cyber-security curriculum library. *Journal of The Colloquium for Information Systems Security Education*, 7 (1), 12 -12 .
- Ozkan, B., Yigit, M., Spruit, R., Wondolleck, & Verónica, B. C. (2020).Modelling adaptive information security for SMEs in a cluster.
- Padilla, T. (2019). Responsible operations: Data science, machine learning, and AI in libraries. OCLC research position paper . Dublin, OH 43017: OCLC Online Computer Library Center, Inc. 6565 Kilgour Place .
- Recognised Universities (2021) [online] Available at: <https://hec.gov.pk/english/universities/pages/recognised.aspx> [Accesed 20 June, 2020].
- San Nicolas-Rocca, T. ,& Burkhard, R. J. (2019). Information security in libraries: Examining the effects of knowledge transfer. *Information Technology & Libraries*, 38 (2), 58–71 .
- Singh, A. K. (2019). Digital library and its security issues: An overview. *Journal Current Science*, 20 (1), 13. Retrieve from <http://www.ijournal.scienceacad.com> .
- Singh, V. ,& Margam, M. (2018). Information security measures of libraries of central universities of Delhi: A study. *DESIDOC Journal of Library & Information Technology*, 38 (2), 102–109 .
- Velte, A., & Wikle, OM. (2020a). Scalable born-digital ingest workflows for limited resources: A case study for first steps in digital preservation. *preservation. Digital Tech- nology& Culture*, 49 (1), 2–13. 10.1515/pdte-2020-0004 .
- Velte, A., & Wikle, OM. (2020b). Scalable born-digital ingest workflows for limited resources: A case study for first steps in digital preservation. *Preservation, Digital Tech- nology& Culture*, 49 (1), 2–13. 10.1515/pdte-2020-0004 .
- Wendzel, S., Levy-Bencheton, C., &Caviglione, L. (2020). Not all areas are equal: Analysis of citations in information security research. *Scientometrics*, 122 (1), 267–286. 10.1007/s11192-019-03279-6 .
- Zhang, L. (2019). Blockchain: The new technology and its applications for libraries. *Journal of Electronic Resources Librarianship*, 31 (4), 278–280 . 8