Gateway Information Journal
G I J

Journal homepage: https://www.gatewayinfojournal.org/

Vol. 20(1) June, 2019

ISSN: 1119–6041

# Are There Threats to Information System Security? A Focus on University Libraries in South-West, Nigeria

**Benedict O. I. Okike**
F. S Idachaba Library
University of Agriculture, Makurdi Benue State, Nigeria
ben16server@gmail.com bensoft15@gmail.com

and

**'Niran Adetoro**
Department of Library and Information Science
Tai Solarin University of Education, Ijagun
niranadetoro@gmail.com.

## Abstract

*Security of data is a key component of information systems while threats to information systems are major challenges especially as the society is largely dependent on Information and Communication Technologies for running its daily activities. This study investigated threats to information systems security in three purposively selected university libraries in South-West, Nigeria. Total enumeration technique was used to capture 48 librarians using a combination of a structured questionnaire which elicited information on threats to the library's information systems and features put in place to protect them; and an interview schedule which was the basis for interviewing librarians specifically in charge of information systems. Total of 42 questionnaires were correctly filled and returned at 88% response rate. The study revealed that librarians had witnessed threats on their information systems. Malware was the major threat to the database/OPAC system (62%), mean ($\overline{x}$) = 2.64; similarly Malware (Virus and Worms) (60%), mean ($\overline{x}$) = 2.62 is the major threat to the operating systems across the selected universities libraries. Furthermore, the study revealed that all the university libraries had high password protection; software updates, firewall, audit and accountability trail on their systems but access control of the information systems was relatively poor. The paper concludes that the university libraries are not immune to attacks as there are threats to the information systems. The study recommends periodic deployment of new protective means, use of telecommunication systems and employment of in-house experts to secure systems and guide against the dire consequences of data loss and destruction.*

**Keywords:** Information System Security, Information Systems, Threats, University libraries, Nigeria

## Introduction

The core value of any information system is the data contained in it. The security of data in today's digital environment is critical to the sustainable existence of any information system. Threats to information systems are a major challenge especially as the society is largely dependent on Information and Communication Technologies (ICTs) for running of its daily activities. A threat can be caused by internal, external or both external and internal entities. Threat is described as the capability of an adversary to attack a system. According to Jouini et al. (2014), threats are techniques that attackers use to exploit the vulnerabilities in your system components. These vulnerabilities consist of weaknesses in a system which can be exploited by the attackers that may lead to dangerous impact. When vulnerabilities exist in a system, a threat may be manifested via a threat agent using a particular penetration technique to cause undesired effects. Alhabeeb et al. (2010) note that in order to find these threats, threats sources and specific areas of the system that may be affected should be known, so the information security assets can be protected in advance.

The extent to which an information system is secured plays an important role in protecting data and information assets of an organization as there are often news about system security incidents, such as defacement of websites, server hacking and data leakages. A secured information system protects information or data from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction (Omosekejimi et al. 2015; Ahmad and Maynard, 2014). Indeed, it is the protection given to intellectual assets of organizations. In this regards, information security plays an important role in protecting the assets of an organization from all threats. Safianu et al. (2016) point out that regardless of the countlessly introduced technological solutions aimed at addressing system vulnerabilities, the human factor is still of greater threat to systems security. It therefore suggested, for information and data breaches to be curbed, organizations must adopt a holistic security framework that incorporates the human factor.

Relative to the computer security, Thanuskodi (2013) posits that information security is not just computer security rather; information security includes issues such as information management, information privacy and data integrity whereas computer security relates to securing computing systems against unwanted access and use. Information security has to with the hardware and software solutions which many organization focus on forgetting system users which is "peopleware" out of the equation (Safianu et al., 2016). System security and data protection go hand in glove, in this case users must be protected, their privacy and confidentiality as well as their electronic devices. On the other hand, there is the need to protect the digital content itself and the electronic infrastructure from abuse or misuse (Liu and Cai, 2013). The security development process requires thorough understanding of systems assets, followed by identifying different vulnerabilities and threats that can exist. It is necessary to identify what the system assets are and what the assets should be protected against (Abomhara and Køien, 2015). In addition, understanding potential attacks allows system developers to better determine where funds should be spent.

Libraries and information centers globally have had their share of threats and breaches to their information systems. System security weaknesses in digital libraries, coupled with attacks or other types of failures had led to confidential information being inappropriately accessed, or loss of integrity of the data stored. (Fox and El-Sherbiny, 2011). Information security system does not only ensure that library patrons are provided access to information but also meant to maintain and monitor the library's hardware, software, and security, guided by documented policies and procedures (Ismail and Zainab, 2013). Ismail and Zainab (2011) have argued that libraries should maintain the privacy of their information assets such as the library's financial information, patrons' circulation information, and passwords used to access the library systems. That patrons should be given appropriate access to the library computers, web sites, databases, and servers based on the principle of least privilege, which refers to only the privileges that they need to perform their specific jobs or tasks in order to protect data integrity from any breaches.

Information systems have become an essential element of libraries. As patrons are using library systems, a large amount of transaction data about users is being recorded and often stored in the systems. This development has severe implications for the security of user data. Not only intruders and criminals can try to gather confidential data, but also government agencies can make inquiries about library users (Rubel, 2014). The security of user information is an important issue in libraries because it bothers on the privacy and confidentiality of the user. However, confidentiality which is the right of library users in their research and library transactions is meant to be kept private. In the delivery of library services, patrons have the rights to their research and library transactions which is meant to be private. In order to maintain the security of user information, there is the need to have a strong and secured network.

In an African setting such as Nigeria, library computers and information systems are not safe, 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 especially in academic libraries, indeed in university libraries where the student are comfortable and dexterious using technology and have shown tremendous ability to manipulate systems to their advantage. There are criminals who specialise in targeted attacks, making it more difficult to handle the risk with the traditional antivirus systems. (Zimerman, 2009). Hackers, Viruses, Worms, and Trojan horses are external extrusions which libraries should be able to handle (Al-Suqri and Akomolafe-Fatuyi, 2012).

Information security incidents occur as a result of employees' failure to observe work procedures according to information security guidelines, it is important for libraries to identify and employ measures that facilitate employee's compliance with suggested guidelines (Spears and Barki, 2010). Libraries are to implement technical measures such as policies, procedures, safeguards and countermeasures to mitigate threats to information security. However, technical measures are insufficient as long as employees are not aware of potential security risks. Information systems security begins and ends with the people within the organisation and with the people that interact with the system, intentionally or otherwise. Abomhara and Køien (2015) identified most commonly known threats as Denial of Service (DoS), physical attacks, malware, password cracking, intrusion, packet sniffing, impersonation, external hacking and attacks on privacy. Subashini and Kavitha (2011) argue that security is one of the major issues which reduce the growth of cloud computing as complications with data privacy and data protection continue to plague the market. Nigerian university libraries in the last decade have deployed information systems in their operations, notably networked systems, database systems, operating systems, physical security systems and the Online Public Access Catalogue (OPAC). It is not common to find all these systems in the libraries however the authors selected those libraries that have these systems in place and has deployed some form of security to protect the systems. In this study, we examine whether there are threats to five basic information systems in some Nigerian University libraries; are there protections against these threats in terms of the security features built into the systems.

## Problem Statement

Few studies have focused on Information Systems Security in Nigerian libraries and information centers despite the incessant clamour for infusion of information technology in the operations of libraries for improved services on one hand and the actual deployment and use of technology, especially among university libraries. This study attempts to fill this gap. Despite the fact that some university libraries have invested much resource in the area of securing their information systems, they still experience threats, attacks and vulnerability to their systems. A preliminary study found that libraries and information centres still do not understand why unauthorised users have access to their information resources; why they still experience hackers attack and theft of information, why some confidential information get to the public domain, why virus and malware attack their system and most times staff do not give full assistance to their users in terms of the information they are seeking. The threats to Nigerian university libraries Database systems, Network systems, Operating systems, Physical security systems and the Online Public Access Catalogue (OPAC) system are not only real but portend great danger to information services. Secured information system that guarantees the integrity, confidentiality and ownership of information in the libraries is a desired goal.

## Research Questions

i) What are the threats to information systems in university libraries?

ii) What are the systems security features put in place to protect the information systems against threats?

## Methods

The study comprised of 48 librarians of the libraries of University of Lagos, Lagos; Covenant University, Ota and Bowen University, Iwo all in South-west Nigeria. The libraries were purposively selected because they are the ones that have deployed the full complement of information systems that was investigated in this study. All the librarians featured in the survey using total enumeration technique. This was due to the small population of the Librarians. A structured questionnaire was used for the librarians with pre-defined questions which elicited information on the possible threats to the library's information systems as well as the security features put in place to protect the systems. The questions (twenty items in all) were generally answered in specified sequence and this was followed by interview schedule section for those librarians specifically in charge of the information systems. The interview schedule has three broad questions which sought information also on the threats and the protection to guard against this. The questionnaire was administered by the researchers and few assistants. The university libraries were visited for distribution and retrieval of the questionnaire for a period of three weeks; the interview for the librarian in charge of the various information systems in the libraries was conducted during the period. Appropriate institutional permission was sought and granted for this exercise.

## Results

We distributed 19 questionnaire to Librarians in University of Lagos, seventeen (17) were returned at 89% return rate, nineteen (19) questionnaire were distributed to librarians in Covenant University, fifteen (15) were returned at 79% return rate while ten (10) questionnaire were distributed to librarians in Bowen University, nine (9) were returned at 90% return rate. In total 42 of the 48 questionnaire were correctly filled and returned at 88% response rate. Librarians who were directly in charge of the information systems were interviewed. 40.5% of the all the librarians surveyed were from University of Lagos; 38.1% from Covenant University while 21.4% were from Bowen University. 38.1% were male while 61.9% were female. Their age ranged from 30-50 years and above; those who were between 30-39 were 45.2% of the total population, those whose age fell within 40-49 constituted 42.9% , while those who were 50 years and above constituted 11.9%.

## Threats to Information Systems.

The respondents were first asked to indicate if they have experienced any form of threat to their information systems and the results revealed that the librarians 73.8% (*n*=31) had witnessed threats on their information systems *mean* $(\bar{x})$ =2.79. Malware was the major threat to the database/OPAC system with a *mean* $(\bar{x})$ = 2.64; (62%). In the same vein, Malware (Virus and

Worms) *mean (x̄)* = 2.62; (60%) is the major threat to the operating systems across the selected universities libraries

The mean and percentage scores for the possible threats to the network system and physical security system were not significant and therefore do not constitute major threats. Although external hacking had *mean (x̄)* = 2.24; (31.7%) while fire and electrical interruption had *mean (x̄)* =2.40; (49.5%).

**Table 1: Threats to the information system security**

| **ITEM** | **SD** | **D** | **A** | **SA** | **Mean (x̄)** | **St.D** |
|---|---|---|---|---|---|---|
| I have witnessed a threat in our information system in the past. | 5 (11.9%) | 6 (14.3%) | 24 (57.1%) | 7 (16.7%) | 2.79 | 0.87 |
| **THREATS** | **SD** | **D** | **A** | **SA** | **Mean (x̄)** | **St.D** |
| **DATABASE/OPAC SYSTEM** | | | | | | |
| Privilege abuse/ breach of confidentiality | 9 (21.4%) | 18 (42.9%) | 11 (26.2%) | 4 (9.5%) | 2.24 | 0.91 |
| Malware | 9 (21.4%) | 7 (16.7%) | 16 (38.1%) | 10 (23.8%) | 2.64 | 1.08 |
| Weak audit trail | 8 (19.0%) | 18 (42.9%) | 13 (31.0%) | 3 (7.1%) | 2.26 | 0.86 |
| SQL input injection | 8 (19.0%) | 18 (42.9%) | 12 (28.6%) | 4 (9.5%) | 2.29 | 0.89 |
| Denial of service | 7 (16.7%) | 18 (42.9%) | 10 (23.8%) | 7 (16.7%) | 2.40 | 0.96 |
| **NETWORK SYSTEM** | | | | | | |
| Packet sniffing | 9 (21.4%) | 23 (54.8%) | 8 (19.0%) | 2 (4.8%) | 2.07 | 0.78 |
| Stack and buffer overflow | 8 (19.0%) | 21 (50.0%) | 11 (26.2%) | 2 (4.8%) | 2.17 | 0.79 |
| External hacking | 8 (19.0%) | 19 (45.2%) | 12 (28.6%) | 3 (7.1%) | 2.24 | 0.85 |
| Theft of service | 10 (23.8%) | 17 (40.5%) | 13 (31.0%) | 2 (4.8%) | 2.17 | 0.85 |
| Disgruntled employees | 10 (23.8%) | 19 (45.2%) | 10 (23.8%) | 3 (7.1%) | 2.14 | 0.87 |
| **OPERATING SYSTEM** | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Impersonation | 11 (26.2%) | 21 (50.0%) | 7 (16.7%) | 3 (7.1%) | 2.05 | 0.85 |
| Password cracking | 12 (28.6%) | 18 (42.9%) | 9 (21.4%) | 3 (7.1%) | 2.07 | 0.89 |
| Breach of integrity | 10 (23.8%) | 15 (35.7%) | 14 (33.3%) | 3 (7.1%) | 2.24 | 0.91 |
| Malware (Virus and worms) | 6 (14.3%) | 11 (26.2%) | 18 (42.9%) | 7 (16.7%) | 2.62 | 0.94 |
| Hardware or software error | 10 (23.8%) | 11 (26.2%) | 13 (31.0%) | 8 (19.0%) | 2.45 | 1.06 |
| **PHYSICAL SECURITY SYSTEM** | | | | | | |
| Neutralizing alerts | 12 (28.6%) | 18 (42.9%) | 10 (23.8%) | 2 (4.8%) | 2.05 | 0.85 |
| Intrusion | 11 (26.2%) | 20 (47.6%) | 9 (21.4%) | 2 (4.8%) | 2.05 | 0.83 |
| Theft | 11 (26.2%) | 16 (38.1%) | 9 (21.4%) | 6 (14.3%) | 2.24 | 1.01 |
| Vandalism | 10 (23.8%) | 19 (45.2%) | 10 (23.8%) | 3 (7.1%) | 2.14 | 0.87 |
| Fire and electrical interruption | 8 (19.0%) | 13 (31.0%) | 17 (40.5%) | 4 (9.5%) | 2.40 | 0.91 |
| **Criterion Mean** | | | | | **2.5** | |

***Mean=2.5 and above is significant*** SD =Strongly Disagree, D = Disagree, A = Agree, SA = Strongly Agree, St.D = Standard deviation

To corroborate these results, an interview was conducted for the systems librarians of the universities selected. Here are their excerpts:

**Excerpts from the interview with the system librarian of University of Lagos**

Have you experienced any form of attack/threat on your information systems? If yes; what type of attack was it?

"*Yes we have experienced an attack on our library portal as a result of that our electronic gateway was not working. The attack affected us in such a way that we lost most of our data*".

Did the attack cost your library much to recover?

"*Yes it did cost us much. We had to pull down everything, pay and re design a new portal which involved much resource. Presently the new portal runs on Linux Red hart operating system as against windows operating system".*

**Excerpts from the interview with the system librarian of Covenant University**

Have you experienced any form of attack/threat on your information systems? If yes; what type of attack was it?

*"We have not really had an attack on our systems. We built a good security on our library information systems more also our systems are running on linux operating system with built in security. Though there was a time we lost most of our data of about 150,000 files due to carelessness from one of our information technology staff that was meant to be backing up all the files but did not do so".*

Did the attack cost your library much to recover?

*"It did cost us much, having lost about 150,000 files. It cost us both man power and cash, we had to reinstall everything and start to catalogue all over again. We had to buy new systems, more servers for back up, we bought inverter. Due to the problem we had, we backup weekly".*

**Excerpts from the interview with the system librarian of Bowen University**

Have you experienced any form of attack/threat on your information systems? If yes; what type of attack was it?

*"Yes we have experienced attacks on our systems both internal and external. Internal attacks were in form of virus and malwares on the personal systems and bugs on the server while external attacks were hacking of our server; they tried to corrupt our server and making it inaccessible for us".*

Did the attack cost your library much to recover?

*"Well, it did not really cost us anything financially since we had IT experts on ground. We had to restore the server and files from our backup file; though in the past we have had a case of natural disaster on our systems".*

Clearly, the three libraries had experienced threats to their information systems in form of malware or virus which resulted in loss of data and at great costs.

**Protection Against threats**

Next, the respondents were asked to indicate the security measures put in place to protect the information systems against threat or attacks. From the various security options puts forward in the survey, the librarians submitted that all the university libraries had password protection 100% (*n*=17) in University of Lagos and Covenant University (*n*=15); 90% (*n*=9) at Bowen University. All the university libraries also had software update protection by 85% (*n*=15), 87% (*n*=13) and 80% (*n*=8) respectively. They all had Firewall in the systems by 65% (*n*=11), 87% (*n*=13) and 70% (*n*=7) respectively. The information systems were also protected with installed audit and accountability trail at University of Lagos 53% (*n*=9); Covenant University73% (*n*=11) and Bowen University 90% (*n*=9). Covenant University 67% (*n*=10) and Bowen University 60% (*n*=6) has access controls in their systems. Only 35% (*n*=6) of the librarians in University of Lagos felt that they had access control on their systems.

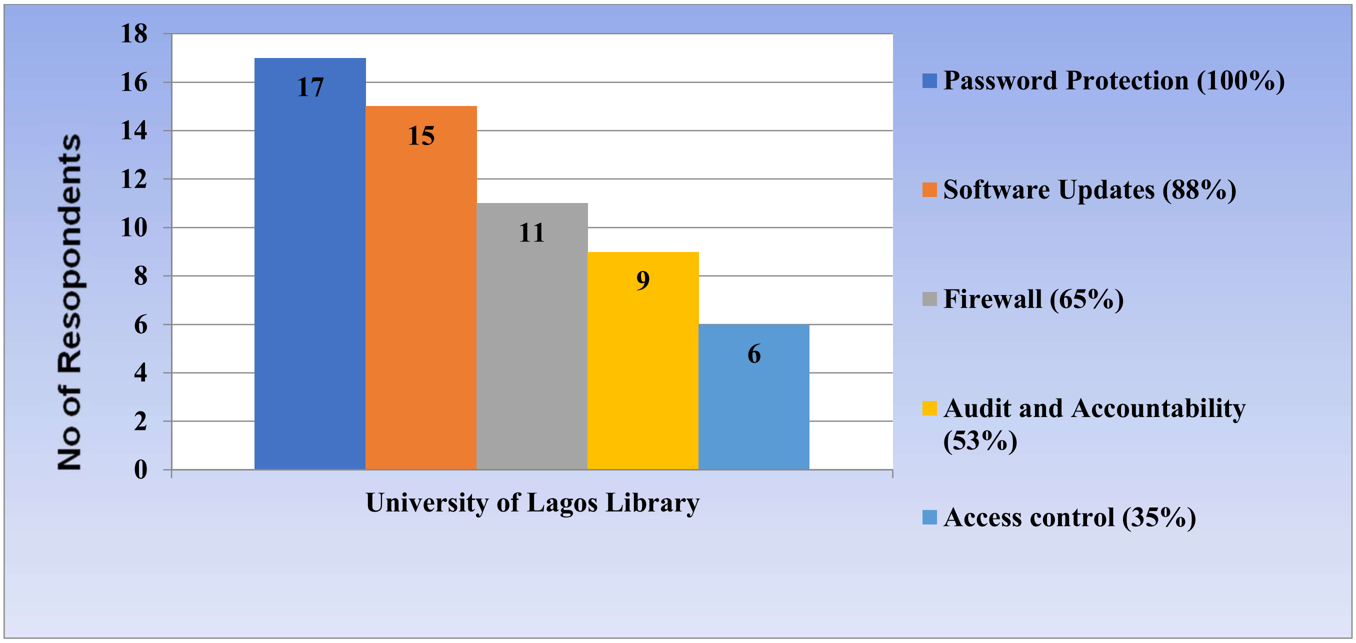

**Figure1**. Security measures to protect Systems against threats at University of Lagos

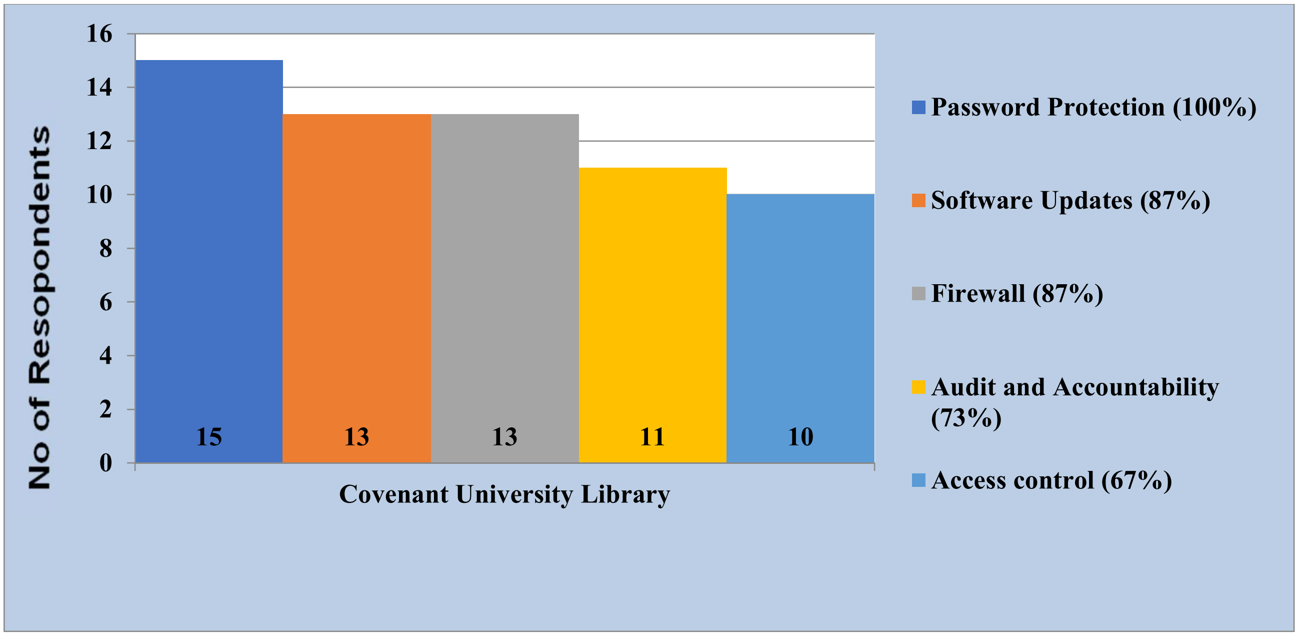

**Figure 2**. Security measures to protect systems against threats at Covenant University

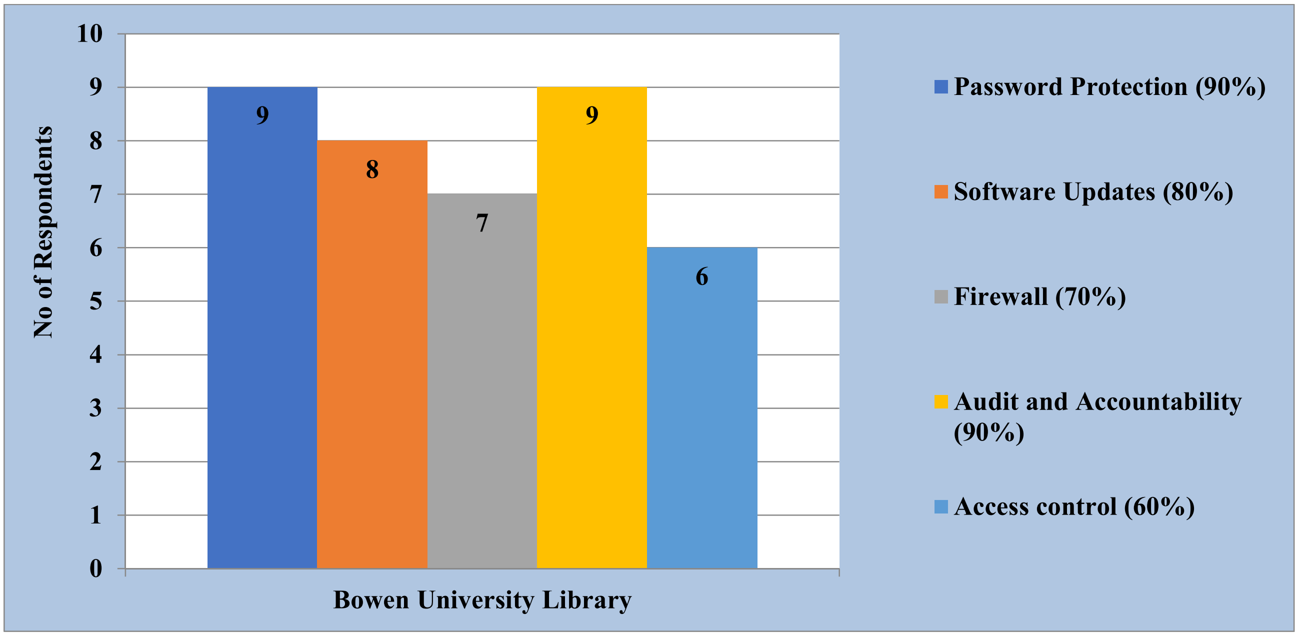

**Figure 3**. Security measures to protect Systems against threats at Bowen University

**Excerpts from the interview with the system librarian of University of Lagos**

Are anti-virus/anti-malware signatures up to date? How often do you update them?

"*We have a centralised server which is where our firewall and anti-virus runs. The anti-virus updates automatically on its own regularly".*

What type of authentication do you use for your systems?

"*We use password authentication for our systems. Before a user can have access to our system s/he must provide an authentication which was given to them by the library, while on the e-library we have a time checker that logs a user out after 2 hours of logging on.*

**Excerpts from the interview with the system librarian of Covenant University**

Are anti-virus/anti-malware signatures up to date? How often do you update them?

*"Yes, we have anti-virus on our systems including the server and they are all up to date".*

Are there physical access controls in place for securing servers and desktop machines.

*"For security reasons our server and Close Circuit Television (CCTV) are on different network. The CCTV is Internet Protocol (IP) based which can be accessed remotely by the system analyst. For controls in securing the server, access to the server room is through biometrics (thumb print).*

What type of authentication do you use for your systems?

*"We use password and biometrics for the systems, 3M and CCTV for monitoring our users while we also have barcode and security chips on our information resources".*

**Excerpts from the interview with the system librarian of Bowen University**

Are anti-virus/anti-malware signatures up to date? How often do you update them?

*"Yes, they are up to date. It updates automatically on its own".*

*"For the server it is not open to all the staff or users. We also have password authentication for the server and personal computer to secure them from unauthorised users".*

What type of authentication do you use for your systems?

“*We use password authentication for our systems. This is done apart from the physical security that we use*”

The interview conducted with the system librarians’ show that the information systems in the three libraries have anti-virus / anti-malware signatures as protection; the servers had firewall and anti-virus. They also have password authentication on the systems. The server at Covenant University is accessible through Biometrics as well as having password.

**Discussion**

In this paper, we investigated the possible threats to information systems of selected university libraries in Nigeria, (those that have deployed the information systems appropriate for this study) and to find out the whether there are security measures put in place by the libraries to protect these systems. Clearly, the finding show that the information systems of the libraries surveyed have come under attack at one time or the other. This was unanimous among the libraries. This is an attestation of the reality of threats to information systems and the critical need for systems to be secured, protected against all kind of threats. Specifically, the information systems in the libraries have come under the threat of malware which includes viruses and worms. It is instructive to note that this is the main threat to both the library database/OPAC and operating systems of the libraries which has led to massive loss of data and huge cost of repairs and replacement nevertheless, the survey revealed that there are other smaller threats; some were internally others were externally induced such as hacking of servers, electrical interruption of systems, and weak audit trail.

The threat of malware is real and concerted efforts should be put in place to mitigate the attack of viruses and worms and the consequences of such attacks. This finding agrees with previous studies (Zimerman, 2009; Ismail and Zainab, 2011). Library computers are not safe, they are physically vulnerable to theft, damage and destruction, but, most of all, they are vulnerable to attacks by a host of malware agents (Zimerman, 2009). This finding has implications for the adequacy of the security of information systems against all kinds of Malware in form of viruses and worms in Nigerian libraries as a whole and by extension African libraries and information centers. Nigerian libraries should not underestimate the threat of viruses; the need for a comprehensive protection of systems is rife. Though libraries in this part of the world do protect libraries against outright theft, vandalism, fire and other possible physical assault on the library and its resources, cyber threats to systems appears to the on the ascendancy in many parts of the world.

Findings reveal that the university libraries had put up similar protective measures against attacks on their systems. All had password protection, software updates, and firewall as well as audit/accountability trail. Some have also put access controls in place to check against threats. The question to be asked now is that in spite of all these protections as claimed, why have the libraries witnessed malware attacks on their systems? Why the servers of some of the libraries' were hacked? These are pertinent questions begging for answers. It is instructive to note that malware are never static and hackers are evolving new tricks and therefore libraries should periodically deploy new protective means to secure their systems and guide against the dire consequences of data loss and destruction.

Despite the foregoing it is important that libraries in Africa also widen the scope of their protective measures and employ the use of telecommunication systems. This confirms the suggestion made by Omosekejimi, Ijiekhuamhen and Ojeme (2015) that necessary telecommunication systems and devices should be made available in libraries to beef up general library security. Furthermore, this study advised libraries to employ competent and experienced in-house computer engineers and system experts who can handle the repairs of systems, telecommunication security systems and devices in case of software failure, hardware breakdown and any form of security threat on the information systems.

## Conclusion and limitations

The information systems in the university libraries studied are not immune to attacks as there are threats to the systems in the libraries surveyed; the major threat being malwares such as viruses and worms. Although these libraries have installed protections and have put up measures to guard against threats, it was evident in the study that there were attacks on the information systems leading to losses at grave costs. The study has shown that the libraries need to do more to protect their information systems against intentional and unintentional attacks. The protection of information systems against attacks is a continuous exercise for libraries; obsolescence of hardware and software poses great danger to information systems security. Libraries need to update their protection measures from time to time to mitigate the ever evolving nature of malwares, viruses and worms and other dangers.

Furthermore, for effective information system security in libraries, librarians and system administrators are expected to re-tool and upskill themselves in the area of information technology in order to achieve optimal security in their information systems. Library administration should regularly train the librarians and system administrators to be up to date on the intrigues of information system security and also acquiring the needed equipment for proper security of their information resources.

This study has some limitations. The small number of libraries surveyed limits the generalizability of the findings, though the reason for this has been explain in the paper.

## REFERENCE

Abomhara, M, and Køien, G.M. (2015), "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks", *Journal of Cyber Security*, Vol. 4 No.1, pp. 65-88.

Ahmad, A. and Maynard, S. (2014), "Teaching information security management: reflections and experiences", *Information Management & Computer Security* Vol. 22 No.5, pp. 513-536.

Alhabeeb, M., Almuhaideb, A., Le, P. and Srinivasan, B. (2010), "Information security threats classification pyramid", *24th IEEE International Conference on Advanced Information Networking and Applications Workshops*, pp. 208-213.

Al-Suqri, M.N. and Akomolafe-Fatuyi, E. (2012), "Security and privacy in digital libraries: challenges, opportunities and prospects" *International Journal of Digital Library Systems (IJDLS)* Vol. 3 No.4, pp. 54-61.

Fox, E. and ElSherbiny, N. (2011), "Security and digital libraries, digital libraries - methods and applications" *Kuo Hung Huang (Ed.)*: InTech.

Ismail, R. and Zainab, A.N. (2011), "Information systems security in special and public libraries: An assessment of status", *Malaysian Journal of Library & Information Science*, Vol. 16 No.2, pp. 45-62.

Ismail, R. and Zainab, A.N (2013), "Assessing the status of library information systems security", *Journal of Librarianship and Information Science,* Vol. 45 No. 3, pp. 232-247.

Jouini, M., Rabai, L.B.A, and Aissa, A.B (2014), "Classification of security threats in information systems", *Procedia Computer Science,* Vol. 32, pp. 489-496.

Liu, W. and Cai, H. (2013), "Embracing the shift to cloud computing: Knowledge & skills for systems librarians", *OCLC Systems & Services: International digital library perspectives,* Vol. 29 No. 1, pp. 22-29.

Omosekejimi, A.F., Ijiekhuamhen, O.P., and Ojeme, T.N. (2015), "Library and information resources' security: Traditional and electronic security measures", *International Journal of Academic Research and Reflection,* Vol. 3 No. 3.

Rubel, A. (2014), "Libraries, electronic resources, and privacy: The case for positive intellectual freedom", *The Library Quarterly* Vol. 84 No. 2, pp.183-208.

Safianu, O., Twum, F. and Hayfron-Acquah, J.B. (2016), "Information System Security Threats and Vulnerabilities: Evaluating the Human Factor in Data Protection", *International Journal of Computer Applications*, Vol.143 No.5.

Spears, J. L., and Barki, H. (2010), "User Participation in IS Security Risk Management", *MIS Quarterly,* Vol. 34 No.3, pp. 503-522, available at: http://130.18.86.27/faculty/warkentin/BIS9613papers/MISQ_SpecialIssue/SpearsBarki2010_MISQ34_3_UserPartic_RiskMgmt.pdf (accessed 12 October 2018).

Subashini, S. and Kavitha, V. (2011), "A survey on security issues in service delivery models of cloud computing", *Journal of network and computer applications* Vol. 34 No.1, pp. 1-11.

Thanuskodi, S. (2013), "Professional competencies and skills for library and information professionals: A present-day scenario", available at: http://www.consalxvi.org/sites/default/files/10-S.%20Thanuskodi.pdf (accessed 12 October 2018).

Zimerman, M. (2010), "Protect your library's computers", *New Library World* Vol. 111 Vol. 5/6, pp. 203-212.