ASSESSMENT OF INFORMATION SECURITY THREATS TO INFORMATION SYSTEMS IN FEDERAL UNIVERSITY LIBRARIES, NIGERIA

By

Ahmed YUSUF, Shuga YUSUF and Hauwau Muhammad ZAYYANA

Abstract

The study assessed information security threat to information syatems in Federal University Libraries in Nigeria with the aim of uncovering the various threats militating against the smooth operations of the system. Sixty four (64) Librarians were randomly selected and surveyed across Federal University Libraries in Nigeria. Questionnaire was used as the instrument for the data collection and bench mark for analysis is determined as positive when the mean is 3.00 and above while a mean of less than 3.00 was regarded as negative. The study found that hardware equipment failure, unauthorized change of software settings, transmission error, data loss due to wrong procedure, power supply failure and employee's misconducts as the major information security threat in the libraries. It was concluded that the libraries will be at risk operating a dysfunctional system which might tamper with its reputation and integrity if the necessary steps are not taken. The study recommended that: the library management should ensure regular maintenance of hardware to eliminate hardware equipment failure and system threats. System administrators should monitor the activities of patrons to avoid unauthorized change of software settings, password attack and installation of unauthorized programs.

Key Words: information, security, threats, libraries

Introduction

Reliance on technology in every aspect of human effort increases the risk to information security (Reid & van Niekerk, 2014; Wiley, McCormac & Calic, 2019). These security risks lead to increasing information security incidents as more organizations are exposed to cybersecurity attacks (Telstra Global, 2017). This is a global issue for CEOs who list cyber risk as their main issue (PricewaterhouseCooper [PwC], 2018). Data breaches and cyberattacks are among the top five social risks in the next decade (The World Economic Forum, 2018; Wiley, McCormac & Calic, 2019). Nigeria is one of the world's weakest nations to digital assaults, Sixteenth most noticeably on the planet in 2016, an improvement from second in 2015. In 2018 alone, about 60% of Nigerian firms endured security breach, and about $270 million is spent on cybersecurity. Regardless of spending great cash on cybersecurity, Nigerian organizations purportedly lost "billions" of naira to information security incidents in 2018. 86% of Nigerian firms experience cybersecurity incident (Adepetun, 2020). More than eight in each 10 organizations from Nigeria are at present encountering cybersecurity attacks. In addition, the influenced information systems are likewise engaging ransomware put at 34 percent; other malware, 43 percent; uncovered information, 57 percent; traded off records, 46 percent and crytojacking, 26 percent (Adepetun, 2020).

Understanding information security threats in information systems helps prevent data loss incidents and their consequences. Every information system in which there is an information security risk must consider the possibility of detecting threats (Hoffmann, Kiedrowicz & Stanik, 2016; Kiedrowicz, M., Napiórkowski, J., & Stanik, J. 2018). The protection of the information system is determined by a set of threats. The ability to prevent the consequences of these threats is determined by the security mechanism of the information

systems (Hoffmanna, Napiórkowskia, Protasowickia & Stanik, 2020). This suggests that information systems need to address new issues such as data protection and security to meet the requirements of the 21st century information environment. This means that in order to remain competitive, information systems need a different perspective on information security and potential threats. An information resource can only be secured if it has assigned security attributes within a certain period of time. Although external factors such as hackers and malware pose great threats to the information security of an information system, the inability to identify security threats by information workers is often viewed as a higher security risk (Willison & Warkentin, 2013; Jaeger, Eckhardt & Kroenung, 2020).

Information security threats in the context of a library mean the need to protect information assets from threats to ensure the confidentiality, integrity, and availability of their information assets. Libraries usually have information resources that need to be protected. The Library Information System contains numerous volumes of resources, services, and user records for library information that can be accessed remotely through the library website. Imtiaz (2001) argues that library service technology should enable online access to information generated around the world and continuous worldwide access to searchable library resources from anywhere, anytime and for everyone. The increasing reliance of libraries on information and communication technologies (ICT) for information management exposes libraries and information centers to various threats. Failure to document and educate librarians about these threats can expose the library to financial and reputation loss. As Zimerman (2010) notes, library computers are physically vulnerable to attacks from malicious agents, including Trojans, viruses, worms, adware, spyware, pornography, keyloggers, password hijackers and theft, damage and destruction. Hackers, viruses, worms, and Trojans are called external threats that libraries must be able to deal with (Al-Suqri & Afzal, 2007). Thus, the availability, integrity and retention of data are key functions of libraries in this digital environment (Brainstorming Report, 2001).

Research Objectives

The general objective of this research to determine the information security threats associated to federal university libraries in Nigeria.

The specific objectives are to:

1. Identify the hardware security threat to information systems in Federal University Libraries, Nigeria.
2. Examine the Software security threat to information systems in Federal University Libraries, Nigeria.
3. Find out the network security threat to information systems in Federal University Libraries, Nigeria.
4. Ascertain the data security threat to information systems in Federal University Libraries, Nigeria.
5. Identify the physical/environmental security threat to information systems in federal university libraries, Nigeria.
6. Find out the human security threat to information systems in Federal University Libraries, Nigeria.

Literature Review

Information security threats in libraries

A threat is a person or opportunity that can negatively affect something (NASA, 2015). Weakness is the type of asset or condition that defines a threat. In terms of structure and system security, threats remain but are minimized by the best possible use of powers and

security methods. Relief is the pressure to prevent the risk from having a negative impact on itself or to completely ignore the damage, or to prevent it when it is inconceivable to improve the speed or adequacy of recovery efforts (Shivram and Davar 2016; NASA, 2020).

The threats to information can cause damages or losses in many ways from small information to entire system destruction. These damages or loses can affect the confidentiality or integrity of data and non-trust on the information system or some other dangerous impact. The information security is vulnerable when computer is stand alone with system software as well as when computer is in network i.e. intranet and internet both. Every day new threats are emerging, making the users of information to be alert and know how to handle the situation effectively (Sattarova, Feruza and Kim, Tao-hoon, 20017). It is necessary to know in advance these threats, their sources and its effect on the information system and to know how to keep the information system more safe and secure and protect it.

Security of information systems

To fully protect the information during its lifetime, each component of information processing system must have its own protection mechanisms. In depth security measures are necessary, where if any measure fails, one can use another defensive measure immediately. All the information security policies and standards have three levels or layers– physical, personal and organizational. Hence there are three types of security controls - administrative, logical and physical (NASA, 2015). The information security essentials explain about the threats to information, security controls, aspects of information security management, factors in digital information security, goals of Information Security and tools for analyzing information security. Looking into the 'Digital India' project a program to prepare India for a knowledge future, the libraries must seriously take into consideration information security management. In libraries we need to handle information systems profoundly besides the print material. This needs us to be aware of information security threats and how to protect the resources from various kinds of threats.

Ryan and Bordoloi (1997) studied how organizations moving from a mainframe environment to a client or server environment evaluate and implement security measures to protect against potential security threats. They found several major security threats, such as: accidental destruction of data by employees; Accidental input by employees of incorrect data; Intentional destruction of data by employees; Intentional penetration by employees of incorrect data; Damage due to insufficient number of backups or log files; And natural disasters (fire, flood, power drainage, etc.).

Pipkin (2000) identified various hazards, including human defects, system failure, natural disaster, and malicious acts. The Centers for Medicare and Medicaid Services (CMS) (2002) classify CMS information systems (SI) into four main groups, namely: environmental or physical hazards; Human hazards; Natural hazards; And technical hazards. Based on their presence and relevance in today's CMS environments, they also rank threats affecting core applications and other human and technological systems. Consider that general support systems are subject to environmental or physical, human, natural and technological hazards. There are threats that can generate and affect system confidentiality, integrity, and availability. Neglect, abuse, theft, vandalism, vandalism or physical intrusion by users are identified as major threats to humanity, compromising the confidentiality of confidentiality, integrity and security of information. Keeping in mind that the main technical risks of privacy, integrity and access to information systems are technical intrusion, unauthorized access to system

resources, in addition to malicious code, database changes, vulnerabilities, system weaknesses, installation errors, and personality changes.

Methodology

Cross-sectional survey was adopted for this study. The method was found appropriate because it is more ideal for studying a spread population and the population of librarians is spread across federal university libraries in Nigeria. Sixty four (64) Librarians were randomly selected across federal university libraries in Nigeria represent the population of this study. Questionnaire was used as the instrument for the data collection. Mean was used to analyze the data collected from the respondents. The bench mark for analysis is determined as positive when the mean is 3.00 and above while a mean of less than 3.00 is regarded as negative.

Results

Table 4.1 Hardware security threat to information systems in Federal University Libraries, Nigeria

Hardware security threats	**SA**	**A**	**SD**	**D**	**U**	**MEAN**
Electromagnetic interference	4	10	9	9	2	2.3
Failure of communication equipments	4	16	5	25	1	3.4
Hardware/ equipments failure	14	10	29	9	2	4.3
Installation/ use of unauthorised hardware	12	18	21	5	6	4.1
Maintenance errors	16	13	19	11	0	3.3
Malware and malicious code	7	6	10	1	4	1.9
Theft of ICT hardware equipments	20	14	0	13	9	3.7

Table 4.1 indicates the different kinds of hardware security threats in the federal university libraries. Hardware equipment failure is reported as the most prevalent threat (4.3) in federal university libraries. Installation/use of unauthorized software (4.1) is the next most threatening to hardware elements of the libraries. Followed by theft of ICT equipments (3.7), then failure of communication equipments (3.4) and finally, maintenance error (3.3). These threats has cost the libraries a lot in term of cost and service delivery since it hindered the smooth operation of the systems.

Table 4.2 Software security threat to Information systems in Federal University Libraries, Nigeria

Software security threats	SA	A	SD	D	U	MEAN
Unauthorised changes to software settings	15	8	20	7	8	3.8
Use of library Internet for illegal or illicit communications or activities	11	14	10	0	12	2.5
User abuse/fraud	5	16	0	9	3	2.2
Weak passwords	2	8	11	1	4	1.7
Installation/use of unauthorised programmes or software	17	10	5	13	5	3.3
Maintenance errors	14	17	10	6	9	3.7
Malware and malicious code	3	6	4	5	8	1.7
Password attacks/sniffing/stealing	10	15	13	12	7	3.8
Software piracy	5	11	7	9	8	2.7
Abuse of computer access control	4	12	6	10	1	2.2
Adware and spyware	8	3	6	9	10	2.4
Failure of system software	10	5	8	2	2	1.8
Cyber-terrorism	3	1	6	2	5	1.1
Hacking/Intrusion/unauthorised access to system resources	2	7	10	3	9	2.1

Table 4.2 shows data on software security threats experienced by federal university libraries. Unauthorized change of software setting and password attack/sniffing/stealing represent the most commonly threat (3.8) in the libraries investigated. Maintenance error (3.7), then installation/use of unauthorized software/programs are also threatening the effective functionality of the libraries.

Table 4.3 Network security threat to Information systems in Federal University Libraries, Nigeria

Network security threats	SA	A	SD	D	U	MEAN
Misrouting/re-routing of messages	0	12	3	1	0	1.1
Packing sniffs	3	7	4	9	1	1.6
Eavesdroping/ wiretapping	5	8	2	7	4	1.7
E-mail attacks /spams/ fraud	15	16	2	13	10	3.7
Hacking/ Intrusion/ unauthorised access	2	7	12	9	1	2.1
IP spoofing attacks	6	3	8	3	8	1.9
Malware and malicious code	4	2	7	6	10	1.9
Transmission errors	10	9	21	11	8	3.9
Weak password	12	10	10	7	13	3.5
Website defacement	3	6	8	10	15	2.8
Wireless network breach	2	7	9	12	3	2.2
Zombie networks	11	8	3	6	10	2.5
Password attacks/sniffing/stealing	5	10	9	21	7	3.5
Probes and scans or unauthorised access to computers, data, services and applications	16	3	10	9	14	3.5
Session hijacking	12	7	15	12	10	3.7
Denial of service attacks (DoS)	20	5	13	11	4	3.5

Table 4.3 indicates the type of network security threats faced by federal university libraries in this research. Transmission error (3.9) have been reported as the most frequent attacks in these libraries. It is evident that most network attacks were due to transmission error. Email attack and session hijacking (3.7), are the next most threatening network security issues in the libraries investigated. Finally, weak passwords, sniffs, probes, scans and denial of service (3.5) represent other types of network security threats in the libraries.

Table 4.4 Data security threat to Information systems in Federal University Libraries, Nigeria

Data security threats	SA	A	SD	D	U	MEAN
Data diddling	2	6	3	9	0	1.3
Data loss due to wrong procedures	15	21	7	12	3	3.9
Data manipulation	3	6	4	9	1	1.5
Delay in updating/dissemination	2	2	7	1	5	1.1
Destruction due to natural disaster	11	10	8	21	7	3.8
Exposure of patrons sensitive data through web attack	8	13	10	12	9	3.5
Impersonation/ social engineering	14	8	12	10	9	3.5
Loss of patron data/privacy ideas	10	21	14	10	1	3.7
Malware and Malicious code	3	6	1	8	0	1.2
Masquerading of user identity	8	20	0	14	12	3.6
Password attacks/sniffing/stealing	17	10	11	6	8	3.5
Phishing/ pharming	3	8	1	4	9	1.7
Theft of proprietary data	15	10	14	0	13	3.5
Unauthorised access	21	12	6	10	1	3.3
Unauthorised data copying	11	10	8	21	7	3.8
Unauthorised transfer of data	1	0	1	5	2	0.6
Unauthorised/accidental disclosure/modifications/alteration of data	12	8	14	9	10	3.5

Table 4.4 ranks the most common data security threats experienced by federal university libraries in Nigeria. These participating academic libraries received an overwhelming numbers of threats on data loss due to wrong procedures (3.9). Destruction due to natural disaster and unauthorized data copying (3.8) each. Loss of patrons data/privacy (3.7) is another type of threat experienced by participating libraries. Masquerading of user identity (3.6) is also a common data security threat in the libraries.

Table 4.5 physical threat to information systems in Federal University Libraries, Nigeria

Physical threats	SA	A	SD	D	U	MEAN
Hazardous material accident	10	8	11	6	7	2.8
Intrusion/ unauthorised access into library building	1	4	7	2	6	1.3
Leaking	4	1	0	5	2	0.8
Natural calamity (e.g. fire, flood, storm, earthquakes or lightning)	13	10	9	5	18	3.7
Power supply failure (e.g. electricity, air-conditioning, water utility)	15	9	18	10	6	3.9
Theft, buglary, sabotage, vandalism or physical intrusions	10	13	9	7	12	3.4

Table 4.5 shows that power supply (3.9) is highest occurring threats in the Federal University libraries. The findings also indicate that natural calamity (3.7) caused by fire, flood, storm or lightning and hazardous materials are common threats associated to the libraries studies. The study also found Theft, burglary, sabotage, vandalism or physical intrusions (3.4) as threatening factors on the physical security of the libraries.

Table 4.6 Human threat to information systems in Federal University Libraries, Nigeria

Human threats	SA	A	SD	D	U	MEAN
Employee misconduct	14	12	9	10	11	3.7
Human errors (data entry errors or carelessness)	8	13	13	9	15	0.4
Online extortion	1	5	7	3	3	1.3
Social engineering	9	9	8	6	12	2.9
Unfaithful patrons	19	11	10	1	14	3.7
Unfaithful staff	12	0	13	11	9	3.0

Table 4.6 rank employees misconduct and unfaithful patrons (3.7) as the most dangerous human-related security threats to Federal University Libraries. In addition to these, the academic libraries are also facing threats of actions of unfaithful staff. This indicates that information security threats in the libraries arises from both internal and external stakeholders.

Conclusion

Based on the above findings, it is worth concluding that federal university libraries in Nigeria are faced with different types of information security threats. Irrespective of types and frequency of occurrence, these treats are posed by internal and external stakeholder. The information security threats have in different ways hindered the smooth operation on the libraries. If nothing is done, the libraries will be at risk operating a dysfunctional system which might tamper with its reputation and integrity.

Recommendation

1. The library management should ensure regular maintenance of information systems to eliminate hardware equipment failure and similar threats.
2. System administrators should monitor the activities of patrons to avoid unauthorized change of software settings, password attack and installation of unauthorized programs.
3. Firewalls and similar security checks should be installed to detect and correct transmission error.
4. The library management should adopt backup strategies to avoid data loss.
5. Generators and solar energy system should acquired by the library management to alternatives to hydro electric power supply.
6. Information security policies should adopt and used to correct employees' misconduct, action of unfaithful staff and patron.

References

Jaeger L, Eckhardt A, Kroenung J, (2020). The role of deterrability for the effect of multi-level sanctions on information security policy compliance: results of a multigroup analysis, Information and amp; Management, doi: https://doi.org/10.1016/j.im.2020.103318

Willison, R., Warkentin, M. (2013)Beyond deterrence: An expanded view of employee computer abuse, MIS Q. 37, 1–20.

Wiley, A., McCormac, A. & Calic, D. (2019) More than the Individual: Examining the Relationship Between Culture and Information Security Awareness, Computers & Security, doi: https://doi.org/10.1016/j.cose.2019.101640

Hoffmann, R., Kiedrowicz, M. & Stanik, J. (2016) Risk management system as the basic paradigm of the information security management system in an organization, MATEC Web of Conferences 76, 04010.

Kiedrowicz, M., Napiórkowski, J., & Stanik, J. (2018) Model of automated control and monitoring system of the current level of information security, Proceedings of the 25th Anniversary Conference Geographic Information Systems Conference and Exhibition.

Hoffmanna, R., Napiórkowskia, J., Protasowickia, T. & Stanik, J. (2020). Measurement Models of Information Security Based on the Principles and Practices for Risk-Based Approach. 1st International Conference on Optimization-Driven Architectural Design. Poland, 2019. Elsevier B.V

Roesnita, I. and Zainab, A.N. (2013). Assessing the Status of Library Information Systems Security. Accepted paper, Journal of Librarianship and Information Science (JOLIS),(UK). (ISI-Cited Publication).

Sancho, J. C., Caro, A., Ávila, M., & Bravo, A. (2020). *New approach for threat classification and security risk estimations based on security event management. Future Generation Computer Systems, 113, 488–505.* doi:10.1016/j.future.2020.07.015

NASA (2020). Information Technology Threats and Vulnerabilities. Retrieved on January 4, 2020 from http://www.hq.nasa.gov/security/it_threats_vulnerabilities.htm.

Shivarama J. & Dawar, V. A (2016). Digital Information Security For Academic Libraries: An Overview

NASA. Information Technology Threats and Vulnerabilities. [Online] [Cited: October 4, 2015.] http://www.hq.nasa.gov/security/it_threats_vulnerabilities.htm.

Jouini, Mouna, Rabai, Latifa Ben Arfa and Ais, Anis Ben. (2014). Classification of security threats in information systems. 5th International Conference on Ambient Systems,

Networks and Technologies (ANT-2014). Procedia Computer Science 32. pp. 489 – 496.

Sattarova, Feruza Y and Kim, Tao-hoon. (2017). IT Security Review: Privacy, Protection, Access Control,Assurance and System Security. International Journal of Multimedia and Ubiquitous Engineering, 2(2), pp. 17-32.