IMPLEMENTATION OF HARDWARE, SOFTWARE AND WORKSTATION INFORMATION SECURITY MEASURES IN FEDERAL UNIVERSITY LIBRARIES OF NIGERIA

By

Yusuf Ahmed
Kashim Ibrahim Library
Ahmadu Bello University, Zaria, Nigeria
e-mail: ahmedyusufkil@gmail.com
Phone no: 08060009103

&
Sanusi L. Saadatu
F.C.T College of Education, Zuba, Abuja
saaswehrt@gmail.com
Phone no:08035042600

&
Joy Emmanuel Omah
Department of Science Education,
Taraba State University, Jalingo
joyomah@gmail.com
Phone no: 08038230502

Suleiman Habiba
Division of Agricultural Colleges
Ahmadu Bello University, Zaria, Nigeria
email: habibasuleiman432@yahoo.com
Phone no. 08068695878

Abstract
The study 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 data collection and bench mark 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 the use of security cables to improve the safety of hardware devices, the use of CCTV in public IT areas and server areas as physical security measures implemented in university libraries. The findings also revealed that use of timer software, cleaning software, web filtering software, library system, and menu replacement software represent the software security measures implemented in university libraries. The study recommended among others implementation of locks and remote mirroring to backup all files in the system, proper implementation of user entrance lock to record and monitor user's security programmes and desktop security programmes.

Keywords: Hardware, Software, Workstation, Information Security, Information Security Measures

Introduction

Information technologies continue to gain relevance in the 21st century libraries and information centers. In this era digital technologies assist in performing library tasks which include data processing, storage, and dissemination. Protecting the information system from various information attacks is a constant challenge facing many libraries (Nasir, Irsha, Hamid and Fahmi, 2019). According to Telstra Corporation (2017), libraries have spent a lot of money protecting information systems from attacks. Despite these efforts, security breaches continue to increase. This problem is compounded by the fact that as technology advances, the types of threats change at the same rate (WEF, 2019). Protecting these systems is more difficult in a university environment where the nature of educational activities to meet the teaching, learning, and research goals determines the different levels of access and availability of both software and hardware. Information systems can be protected by implementing technical and non-technical methods. Technological methods are applied to cryptography, firewalls, authentication methods, and security models to deal with information systems security attacks. On the other hand, the non-technical approach focuses on ensuring the proper implementation of hardware, software, workstations, servers, data, and physical security measures (Workman, 2009).

Information security studies revealed that combination of measures is needed in order to protect information systems (Pattinson, Parsons, Butavicius, McCormac & Carlic, 2016). One of the proposed methods is to ensure proper implementation of information security measures. Studies have suggested the implementation of information security measures, which are the least implemented by libraries (Prince Waterhouse Cooper, 2018). Despite the implementation of security measures, many libraries were unable to reduce security issues to better understand the implementation of information protection measures (Albrichton and Houden, 2009 Reid & Van Niekerk, 2014).

Literature Review

There are many IT security measures that, if properly implemented and managed, have a significant impact on combating cyber terrorism. This includes properly installed, running, and regularly updated firewalls, anti-virus programs for package detection software, and access control lists. However, by far the greatest threat to a security system is that users protect the system accidentally, unwittingly, cheaply, unknowingly, or on a daily basis. Most of the cyber criminals and cyber terrorists do not need the latest software or hardware tools to access the system unless the user's case is Android. Therefore, with clear, well-defined, quality-oriented policies and protocols, and training systems, to establish security as the center of each organization's organizational culture, establish good cyber hygiene for each organization (Shimeal, 2019).

Libraries implement and assist a variety of mechanisms to avoid, mitigate, or reduce information security risks. Although these methods have not been documented or technically created, they do exist informally as a culture of internal security. Control, Precautions, Countermeasures are used to describe the mechanisms used to secure information. Information security countermeasures can also be seen as "measures taken to counter threats". Countermeasures can be classified in a variety of ways. One way is

to characterize them by what they do - preventive action, spy action or corrective action. Countermeasures can also be characterized by type - administrative, logical and physical (McLeith, 2016).

According to Hampshire (2017), there are three main types of hardware, software and workstation countermeasures. Some researchers (Wyant, 2015) believe that security rights are only a technology and method, while others say that informal principles seriously affect employees' information security behavior. Yes, and it is possible to combine informal principles and thereby reduce internal risk. Dr Veiga (2010) has shown that aspects of information security, information security behavior and information security culture are interrelated. In this document, not only the technical and formal procedural principles, but also the informal principles are considered as countermeasures, and the end user's knowledge and emotional aspects of each of these issues are analyzed to identify changes in safety behavior.

White and Pearson (2017) investigated about 200 American industries to ascertain the safety of personal computers in the wake of cyber threats. The research suggested a better counter measure to be activated in the industries. The study also suggested that industries are beginning to incorporate information security plan in their plans.

Haniza (2019) explored adoption rate of information security guidelines and users action. Triangulation was adopted in data collection where experts were interviewed and users were surveyed using questionnaire. The outcome revealed that majority of the respondents claimed adequate awareness and knowledge of the guidelines.

Dionysiou, Kokkinaki and Magirou (2020) studied information security in thirty-three governmental and non-governmental organizations in Europe. The major finding revealed that there is adequate information security countermeasure in the organizations.

Despite the importance of these studies in the context of information security, none of these studies aimed at uncovering issues related to implementation of information security measures in Nigerian Federal universities especially the libraries.

Research Questions

a. What is the level of implementation of hardware security measures in Federal university libraries in Nigeria?
b. What is the level of implementation of software security measures in Federal university libraries in Nigeria?
c. What is the level of implementation of workstation security measures in Federal university libraries in Nigeria?

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. Four hundred and eighty (480) Librarians were randomly selected across Federal university libraries in Nigeria to represent the population of this study. Four hundred and sixteen (416) librarians returned their instruments in usable form. 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 bench mark for analysis is accepted when the mean is 2.50 and above while a mean of less than 2.50 is rejected. The response scale and values assigned is SA= 4 A= 3 D= 2 SDA= 1

Results

Table 4.1: Level of Implementation of Hardware Security Measures

Hardware security measures	SA	A	D	SDA	MEAN
CCTV	158(38%)	179(43%)	33(7.9%)	46(11.1%)	3.0
Visual camera	118 (28.4%)	202(48.6%)	51(12.3%)	45(10.8)	2.9
Magnetic detection device	122(29.3%)	215(51.7%)	31(7.5%)	48(11.5%)	2.9
Digital anti-theft device	104(25.0%)	214(51.4%)	46(11.1%)	52(12.5%)	2.8
Installing emergency power sources	78(18.8%)	191(45.9%)	85(20.4%)	62(14.9%)	2.6
Adopting locks	61(14.7%)	171(41.1%)	105(25.2%)	79(19.0%)	2.4
Security cables	215(51.7%)	120(28.8%)	31(7.5%)	50(12.0%)	3.1
Use of locked cable trays	149(35.8%)	158 (38.0%)	56(13.5%)	53(12.7%)	2.9
Use of anchoring devices	72(17.3%)	166(39.9%)	110(26.4%)	68(16.3%)	2.5
Use of remote mirroring	67(16.1%)	102(24.5%)	148(35.6%)	99(23.8%)	2.2

Table 4.1 shows the various stages of implementation of physical security measures in federal university libraries. The table shows the highest mean, with a statistical mean value of 3.1, representing the security cables used to improve the safety of hardware devices in strategic locations with a statistical mean of 3.0, the use of CCTV in public IT areas and server areas has been found to be a physical security measure implemented in university libraries. It is clear that these two physical security practices have been implemented in these participating university libraries in Nigeria. System electronic anti-theft devices, public IT areas and server areas in strategic locations, with the use of visual camera, magnetic detection system and locked cable trays to improve the security of hardware equipment in strategic locations, public IT areas and server areas (mean = 2.9). (Mean = 2.8), backup power sources and alternative transmission lines (2.6), and metal cages or anchors to improve the safety of physical equipment, respondents indicated that these security measures were implemented but these measures were not regularly reviewed in the respective libraries.

Table 4.2: Level of Implementation of Software Security Measures

Software security measures	SA	A	D	SD	MEAN
Of cleanup software	159(38.2%)	163(39.2%)	18(4.3%)	76(18.3%)	2.8
Use of Anti spyware software	96(23.1%)	194(46.6%)	44(10.6%)	82(17.7%)	2.6
Use of ID management software	85(20.4%)	173(41.6%)	73(17.5%)	85(20.4%)	2.5
Use of Web filtering software	121(29.1%)	204(49.0%)	33(7.9%)	58(13.9%)	2.8
Use of anti-phishing solutions	98(23.6%)	193(46.4%)	40(9.6%)	85(20.4%)	2.6
Use of multi user operating systems	57(13.7%)	152(36.5%)	113(27.2%)	94(22.6%)	2.3

Adoption of user entrance log to record and monitor user logs	56(13.5%)	96(23.1%)	152(36.5%)	112(26.9%)	2.1
Use of desktop security software	71(17.1%)	145(34.9%)	112(26.9%)	88(21.2%)	2.3
Use of distribution agents	87(20.9%)	156(37.5%)	72(17.3)	101(24.3%)	2.4
Use of systems recovery	154(37.0%)	150(36.1%)	31(7.5%)	81(19.5%)	2.8
Use of spam filtering software	186(44.7%)	168(40.4%)	20(4.8%)	42(10.1%)	3.1
Use of timer software	137(32.9%)	194(46.6%)	33(7.9%)	52(15.5%)	2.9
Use of rollback software	69(16.6%)	74(17.8%)	100(24.0%)	173(41.6%)	2.0
Adoption menu replacement software	147(35.8%)	135(32.5%)	67(16.1%)	67(16.1%)	2.8
automatic debugging	163(39.2%)	116(27.9%)	37(8.9%)	100(24.0)	2.7
Single sign on system for user authentication	139(33.4%)	148(35.6%)	65(15.6%)	64(15.4%	2.8

The use of some software security tools in the participating university libraries is confirmed by the responses of the respondents listed in Table 4.2. Respondents stated that the university library had timer software (mean = 2.9) to control how long the user could use the workstation, cleaning software (mean = 2.8) to erase files and settings left by the user, I believe you are using web filtering software to prevent improper access Material or site (mean = 2.8), library system recovery to rebuild and repair your library computer system after a disaster or crash (mean = 2.8)), Menu replacement software that replaces the standard Windows desktop interface and provides control over timeouts, logging, and browsing activities (mean = 2.8) = 2.8), access all computers and systems without the need to enter multiple passwords System single sign-on for user authentication and authorization (mean = 2.8), automatic debugging, regular testing to remove defects in newly developed software or hardware components (mean = 2.7), spyware attacks Anti-phishing solution to prevent (mean = 2.6), anti-spyware software to detect and remove spyware threats (mean = 2.6) Advertising Allows users to reset user passwords and their own passwords Qualification management software that automates management tasks such as (mean = 2.5). However, these software security checks have never been reassessed by these university libraries. The findings also revealed that use of timer software, cleaning software, web filtering software, library system, menu replacement software represent the software security measure implemented in university libraries.

Table 4.3: Level of Implementation of Workstation Security Measures in Federal University Libraries, Nigeria

Workstation security measures	**SA**	**A**	**D**	**SD**	**MEAN**
Virus protection programs are installed for web browsers and email.	98(23.6%)	193(46.4%)	65(15.6%)	60(14.4%)	2.7
Configuration settings programs are installed	104(25.0%)	182(43.8%)	60(14.4%)	70(16.8%)	2.6

Installation of security software programs	87(20.9%)	152(36.5%)	98(23.6%)	79(19.0%)	2.5
use of user identification and authentication before login	91(21.9%)	187(45.0%)	71(17.1%)	67(16.1%)	2.6
All office productivity software and browsers for the workstations/laptops are configured to receive updates in a timely manner.	66(15.9%)	109(26.2%)	150(36.1%)	91(21.9%)	2.2
Use of firewall.	66(15.9%)	112(26.9%)	121(29.1%)	117(28.1%)	2.2
The computer's BIOS are secured in order to create a secure public access computer.	137(32.9%)	133(32.0%)	43(10.3%)	103(24.8%)	2.6

It is clear from Table 4.3 that virus protection programs have been installed for web browsers and this email has the highest mean value with value of 2.7. The respondents reported that their educational libraries followed configuration programs for web browsers and e-mail (i.e = 2.6), and before logging into the library workspace, laptop screen savers, and library User ID and visual verification required Network or Campus Network (Mean = 2.6) Respondents confirmed that the computer's BIOS is secure enough to create a secure public access computer (Mean = 2.6), and security software programs for web browsers and email (Mean = 2.5). However, at the time of this survey, there has been no change in the use of workplace security tools. This finding revealed that virus protect and configuration software, library ID user, visual verification and computer BIOS are installed as counter measures in then libraries systems.

Conclusion

Based on the above findings, it is concluded that Federal university libraries in Nigeria are faced with various information security threats. Irrespective of types and frequency of occurrence, these threats are posed by internal and external stakeholders. The information security threats have in different ways hindered the smooth operation of the libraries. Without necessary measures, the libraries will be at risk of operating a dysfunctional system with the resultant negative consequences.

Discussion

The study was guided by three research questions. Research question sought to discover the level of implementation of hardware, software and workstation security measures in the area covered.

The study revealed that the use of security cables to improve the safety of hardware devices, CCTV in public IT areas and server areas has been found to be a physical security measure implemented in university libraries. Meaning that, acquisition of hardware devices for library operation without adopting and implementing the right security measures will certainly lead to worthless investment. Implementation of the right information security measure will help to prevent third party intrusion and increase the system durability. This finding is in agreement with that of Shimeal (2019) who believed that to avoid, reduce or mitigate risks related to information security; libraries must implement and maintain various mechanisms. Even if those mechanisms are not documented or established by technical means, they should exist informally as an internal security culture. Research question 2 was answered to find out the implementation level of software security measures in the study area. The findings also revealed that use of timer software, cleaning software,

web filtering software, library system, menu replacement software represent the software security measure implemented in university libraries. This shows that the libraries studied have implemented different types of software security measures to protect their valuation assets (information content) from destruction. This finding contradict that of White and Pearson (2017) who believed that believed that university libraries in Nigeria are yet to adopt and implement information security measure for their software.

Research question 3 was answered to find out the implementation level of workstation security measures in the study area.

This is not surprising since security software programs such as anti-virus, anti-spyware and anti-adware software programs are widely available and are nowadays commonly used to detect and eliminate malicious programs. This finding revealed that virus protect and configuration software, library ID user, visual verification and computer BIOS are installed as counter measures in then libraries systems. This result agrees with the findings of Dionysiou, Kokkinaki and Magirou (2020) who believed that there are adequate workstation security measures in the university libraries.

Recommendations

1. The library management should ensure full implementation of locks and remote mirroring to backup all files in the system.
2. System administrators should ensure proper implementation of user entrance lock to record and monitor users' security programmes and desktop security programmes. Rollback security should be implemented to keep track of changes made to the system.
3. The library management should ensure full implementation of firewalls as workstation security programmes.

References

Albrechtsen, E & Hovden, J (2009), "The information security digital divide between information security managers and users", *Computers & Security*, Volume 28, Issue 6, pp. 476-490.

Da Veiga, A. (2018). An approach to information security culture change combining Information & Computer Security, 26(5), 584-612.

Da Veiga, A., & Eloff, J. (2010). A framework and assessment instrument for information security culture. *Computers &Security*, 29(2), 196-207.

Dionysiou, I. Kokkinaki, A. and Magirou, S. (2020). Preliminary Survey Results On IT Security Practices In Cyprus Private And Public Sectors. MCIS 2010 Proceedings. Paper 25. Retrieved December 12, 2010, from http://aisel.aisnet.org/mcis2010/25.

Hampshire, E. (2017), "Research on usability in information security", Computer Fraud & Security, Volume 2007, Issue 6, pp. 8-10.

Haniza S. (2019). *Users' perception of the information security policy at Universiti Teknologi Malaysia. Master's thesis, Universiti Teknologi Malaysia*, Faculty of Computer Science and Information System.

Herath, T & Rao, H. R. (2009), "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness", *Decision Support Systems*, Volume 47, Issue 2, pp. 154-165.

McIlwraith, A. (2016), Information security and employee behaviour: how to reduce risk

Nasir, Arshah, Hamid, & Fahmy. (2019). An analysis on the dimensions of information security culture concept: A review. *Journal of Information Security and Application*, 44, 12-22.

Pattinson, M., Parsons, K., Butavicius, M., McCormac, A., & Calic, D. (2016). Assessing information security attitudes: A comparison of two studies. *Information and Computer Security*, 24(2), 228-240.

Pricewaterhouse, C. (2018). Key findings from the Global State of Information Security Survey 2018. Revitalizing privacy and trust in a data-driven world. Retrieved from pwc.com/us/en/services/consulting/cybersecurity/library/information-securitysurvey/revitalizing-privacy-trust-in-data-driven-world.html 21/2/2021

Reid, R., & van Niekerk, J. (2014). Brain-compatible, web-based information security education: A statistical study. Information Management & Computer Security, 22(4), 371-381.

Schlienger, T., & Teufel, S. (2003). Analyzing information security culture: Increased trustby an appropriate information security culture. Database and Expert Systems Applications, 2003. Proceedings. 14th International Workshop (pp. 405-409). Prague: Czech Republic.

Shimeal, T. J. (2019), "Common sense guide to prevention and detection of insider threats 3rd edition – Version 3.1", Carnegie Mellon University.

Telstra Corporation. (2017). Telstra Cyber Security Report 2017. Retrieved from telstraglobal.com/images/assets/insights/resources/Telstra_Cyber_Security_Report_2017_-_Whitepaper.

through employee education, training and awareness, Gower Publishing Company.

WEF (2019) The global risks report 2019. 14th edition. world economic forum. Geneva. http://www3.weforum.org/docs/WEF _ Global _ Risks _ Report _ 2019. pdf . Accessed 13 March 2019.

White, G.W. and Pearson, S.J. (2017). Controlling corporate e-mail, PC use and computer security. Information Management and Computer Security. 9(2):88 – 92.

Wiant, T. L. (2015), "Information security policy's impact on reporting security incidents", Computers & Security, Volume 24, Issue 6, pp. 448-459.

Workman, M (2009) "A field study of corporate employee monitoring: Attitudes, absenteeism, and the moderating influences of procedural justice perceptions", *Information and Organization*, Volume 19, Issue 4, pp. 218-232