MANAGEMENT OF LIBRARY AND INFORMATION CENTRES IN THE ERA OF GLOBAL INSECURITY

A FESTSCHRIFT IN HONOUR OF

PROF. (SIR) MATTHEW IDOWU AJIBERO (KSM)

MANAGEMENT OF LIBRARY AND INFORMATION CENTRES IN THE ERA OF GLOBAL INSECURITY

A Festschrift in Honour of

PROFESSOR MATTHEW IDOWU AJIBERO

Editors

Professor Abdulwahab Olanrewaju Issa

Dr. Abdulsalam Abiodun Salman

Dr. Tunde Kamal Omopupa

Dr. Lambe Kayode Mustapha

Dr. Shuaib Agboola Olarongbe

Department of Library and Information Science,
Faculty of Communication and Information Sciences,
University of Ilorin, Ilorin, Nigeria.

Management of Library and Information Centres in the Era of Global Insecurity

A Festschrift in Honour of

PROFESSOR MATTHEW IDOWU AJIBERO

First Published in 2020
By
Tim-Sal & Bim Publishing Ltd.

ISBN: 978 - 978 - 57021 - 9 - 4

Printed in Nigeria by:
TIM-SAL & BIM PUB. LTD.
Ilorin.
Tel.: 08077787630

INFORMATION SECURITY AWARENESS POLICY ON COMPLIANT BEHAVIOUR OF INFORMATION USERS IN ACADEMIC LIBRARIES

By

OJO, JOSHUA ONAADE, *Ph.D.*
University Main Library, Technical Services Department,
Acquisitions Section, University of Lagos, Akoka, Yaba.
onaade@gmail.com

BAMGBOSE, AUGUSTINE ADEOYE
College of Medicine Library, E-Resources Department,
Lagos State University, Opposite Police College, Ikeja
&
GBENU, SARAH
Lagos State University, University Library, Technical Services Department,
Cataloguing and Classification Section, Ojo.

ABSTRACT

This paper examined the information security awareness policy on compliant behavior of information users in academic libraries in Nigeria. The study discusses and x-rayed the rationale for information security awareness policy in tertiary institution of higher learning and the need for compliant among the users for the purpose of adequate protection of the various information resources garnered for years for the purpose of academic attainment. Objectives of the study include; to identify the level of information security awareness policy of librarians in academic libraries users' compliant behavior and factors that influence information security awareness policy in academic libraries' information services. It highlights the emergent of information communication technology to be used as device to guarantee the three main elements of information security such as confidentiality, integrity and availability. The new dimension has given impetus for acquisition, organization, processing and dissemination of information in the academic libraries. It identifies the desire of every library to have maximum patronage from its users, and there is need to have adequate security measure in place to safeguard the avalanche of information resources provided for the various strata of members of community of users. The entire measures put in place the problem of implementation and non-compliant behavior by various categories of users have been the bane of development of information security awareness policy due to non-charlatan attitude of users in academic libraries. It concludes that challenges not withstanding issues associated with information security awareness policy on compliant behavior of information users in academic libraries and particularly compliant behavior of information users, all personnel, who are mainly the librarians, library officers and library management should be able to understand the information security policies of their employers.

Keywords: Information, Security awareness, Policy, Compliant, Academic libraries, Confidentiality

INTRODUCTION

The 21st Century has continued to witness the era of Information Technology and

Information which is regarded as the key resource for the overall development of persons or a whole nation. Information is knowledge, security and is power seen as a basic ingredient for personal, social and national development. The introduction of Information and Communication Technology (ICT) has brought a new dimension in the generation, acquisition, organization, processing and dissemination of information in the academic libraries. Information security awareness policy device is used to guarantee the three main elements of information security. They are confidentiality, integrity, and availability. The world today is about knowledge acquisition which is resided in the library of the various types. Uzuegbu, et al (2013) posited that publication and other works of knowledge hitherto held in library shelves are now domiciled on the cyberspace and digital networks, some as subject or professional gateways and others aggregated database, accessible via the Internet or as files installable on computer desktops that can be shared through local and wide area networks. Whichever case, such products are what informational professionals have called electronics resources.

Nowadays, the holdings of academic libraries are merely incomplete where there are no electronic resources. The satisfaction of the informational needs of each individual user is important both in the traditional form of attendance and in the form that is required (virtually) in the daily life of academic libraries. Therefore, it becomes extremely important to control and reduce technical incidents and security, among other factors, in order to ensure the operation of the network at acceptable levels of performance as well as to keep your equipment with specialized software and applications to facilitate the communication and optimize the flow of information and knowledge, thus allowing the increase of efficiency and conditions of excellence of the information stored in the system used by the libraries, whether in the field of research, teaching, extension, services or institutional management (Lima, et al 2014).

Ogunsola (2011) asserted that "traditionally libraries were collections of books, manuscripts, journals, and other sources of recorded information. In the last 50 years, libraries have increasingly developed into a provider of information resources and services that do not even require a building" (p. 34). The library's traditional lasting objective is to provide access to relevant information resources. The aim of this is to give high value to the needs and expectations of users. Generating and sharing information is useless, if there's no way to locate, filter, organize and access it. Traditionally librarians are in the forefront of information dissemination and they will continue to be there (Ramos, 2007). Libraries collect, stock, process, organize, disseminate and distribute information/knowledge recorded in documentary and non-documentary sources/formats. Since knowledge and information are so vital for all round human development, libraries and other institutions that handle and manage knowledge and information are indeed invaluable in national security.

According to John (1998, p. 23) "of all the roles that librarians and libraries play two are critical to modern society as we know it. The first is the role of the library as the place where the information seeker can access information without restriction - the access role. The second role has been the world-wide effort of libraries to archive, protect and provide

ongoing access to information and the world's cultural heritage for the long term - the preservation role. These two fundamental roles have differentiated libraries from all other institutions" (p.26). In this vein to propose that libraries are "in the midst of a revolutionary phase, with new assignments crowding the librarian's agenda, is to state the obvious" (Mokogwu, n.d cited in Ossai-Ugbah, 2013, p.13). With all these information resources put in place in divert formats it is imperative to ensure adequate security for protection to guide against theft and any other means of stealing or vandalizing by users whose majority are students. It might obvious to say that in this part of the world security awareness is an often-overlooked factor in an information security program. While organizations expand their use of advanced security technology and continuously train their security professionals, very little is used to increase the security awareness among the normal users, making them the weakest link in any organization (Aloul, 2012).

Library and information security is the method which has been used to conserve and preserve the integrity, availability and confidentiality of electronic information. Security control reduces the impact or probability of security threats and vulnerabilities to a level acceptable to the organisation. Information security is as important as it has ever been, but the challenges to determine the factors contributing to information insecurity prove to be of complex nature. In libraries, information systems (IS) are widely used to deliver services and collections to local and remote patrons. This is typically done in order to control access to the information in different ways, depending on its importance, its sensitivity, and its vulnerability to theft or misuse. Most of the information on security issues relies on physical devices. The device is used to guarantee the three main elements of information security. They are confidentiality, integrity, and availability. Discussion about these three elements, how equipment can protect data in the system or database, how the firewall protects to prevent outside attacks, how secure are the software or applications used to dispel hackers, and why technology cannot ensure against humans making mistakes.

This forms another part of the information security issue, namely information security awareness. Information security awareness (ISA) is referred to as a state of consciousness and knowledge about security issues and is frequently found to impact security compliant behavior. According to Boyce and Jennings (2002), security awareness occurs when a user understands the security policies, procedures, and practices, in order for them to make sound judgments when a potential security issue occurs, in the absence of further guidance. The aim of information security awareness is to improve information security by enhancing and adopting security policies and countermeasures (ENISA, 2006), improving IS users' security behaviour (Puhakainen, 2006), or altering work routines, so that good security habits are applied (Hansche, 2001). However, to date little is known about the factors influencing ISA and its mediating effect on behavior.

STATEMENT OF THE PROBLEM

It is the desire of every library to have maximum patronage from its users, and when this happen there is need to have adequate security measure in place to safeguard the avalanche of volume of information resources provided for the various strata of members of community of users. It is germane for library management to ensure that various forms of

protection are put in place to ensure that those information resources are well protected and ensure that users are aware of information security policy that will stipulate the details and manners in which those resources are well protected by disseminating such policy adequately during orientation and library instruction to newly admitted students and also embedded in the library handbook. With these entire measures put in place the problem of implementation and non-compliant behavior by various categories of users has been the bane of development of information security awareness policy because of non-charlatan attitude of users in academic libraries.

OBJECTIVES

To identify the level of information security awareness policy of librarians in academic libraries users compliant behavior;

i. To identify the factors that influence information security awareness policy in academic libraries information services;
ii. To identify the level of compliance with rules and regulations in the academic libraries services;
iii. To highlight challenges of information security awareness policy and compliance in academic libraries information services.

LITERATURE REVIEW

The best approach to guide information resources in the academic libraries is to ensure that policy for security issues are well enshrine in the policy documents approved for the setting up the library. University senate committee in charge of the library development is to review such policy guidelines at appropriate time by reflecting on what obtains in developing countries. Information resources that comprises of textbooks, journals databases are very expensive through high subscription rate periodically, most of these resources are loaded in computers and workstations as the case may be and housed in conducive environment devoid of act of vandalism, it is imperative that such expensive information resources should be well secured. Information users who are mostly students are the target when it comes to mutilation, theft, and vandalisation of books and journals, the first approach to guide against this would during orientation and teaching of users' education as general study course at the beginning of a new session.

Succinctly, the essence of such course is to introduce the students who will later become the users of the materials, that information security is means and ways of protecting data from unauthorized access, change, misuse, loss and ensures its availability whenever required. At the beginning, information security was focused mainly on technical issues and the responsibility was left to technical experts (Von, 2000). University libraries face a number of security challenges with their collections (both print and non-print. According to Maidabino (2011) asserted that library collections constitute the bedrock for services provided to the community and serve as important assets to the library. Uzuegbu and Caroline (2013) developed a model named LISSAM (library information systems security assessment model), consists of five components: information security policy, technological security foundation, administrative tools, methods, procedures and control and awareness

creation. Ma Jun-tao, et al (2010)stressed upon the network security risks in digital medical libraries and their effective preventive measures, and pointed out the major flaws in their CD-ROM and full-text databases and their preventive measures.

Suffice to say that information is a vital asset to any organisation and this is especially so in a knowledge-driven organisation such as we have in some of our tertiary institutions in Lagos-State, where information will relate to learning and teaching, research, administration and management. Library management committee's policy is concerned with the management and security of the University's information assets -an information asset is defined to be an item or body of information, an information storage system or an information processing system which is of value to the university and the use made of these assets by its members and others who may legitimately process university information on behalf of the university. This overarching policy document provides an overview of information security and lists a hierarchical set of policy documents (sub-policies) which taken together constitute the Information Security Policy of the University (University of Bristol, 2019). However, an effective Information Security Policy provides a sound basis for defining and regulating the management of information systems and other information assets. This is necessary to ensure that information is appropriately secured against the adverse effects of failures in confidentiality, integrity, availability and compliance which would otherwise occur.

It is important that community of library users are aware of the various policy, rules and regulations that abide in the university to guide against various facets of information resources that are put in place for students and researchers. It is a good thing to put the policy in black and white paper it is another thing for the users to know that it is in existent. Mentioned have been made that awareness should start from user education as part of their courses, the reaction of students to these in terms of their behavior requires that adequate security awareness is needed information of advocacy and sensitization. According to Straub (1990) cited in Kamal, Zaini and Shahibi (2012), policy regarding the proper and improper use of information systems needs to be established. The more detailed that these policies are, the greater the deterrent impact on unacceptable systems use is. After these policies are in place, the administrator should educate the users about acceptable information security behaviour. There are many ways to educate users. As Solms and Solms (2004 cited in Kamal, et al 2012) stated that policies should provide guidance to employees and partners, to how they should act and behave in order to be in line with management's wishes.

Academic libraries with clear guidelines in their policy manual, information system would be strengthened through the information security, thus this will define other series of polices within the university system, interestingly this does not mean that these policies would be obeyed by university staff both academic or non-academic including the students who formed bulk of library users. In this case the library management must ensure that proper information literacy education process that will ensure appropriate behavior. There is need for the understanding of the policy that has been put in place to guide and ensure the adequate security of information resources. Such that the community of users that

majorly are students would know how handle such materials that most of them are not easy to come by with respect to purchase, scarcity, high subscription rate and latest publication for accreditation purposes in the life of accrediting of a particular course which might be germane to the overall development of such university. The level of compliance with library rules and regulations by

Students in tertiary institutions in Lagos has some mixed feelings, reported cases of books theft, damages, mutilation and mishandling inform of vandalisation are abound everywhere and is not encouraging. Study has revealed that a significant number of students were aware of the rules and regulations in the library as well as punishment and sanctions are given to offenders (Ameyaw, 2018). Users should have it at the back of their mind that academic libraries are established to serve the needs of their parent institution; thus, to support learning, teaching and research needs of their clients in the academic community. These libraries are perceived all over the world as a backbone of the university, because of this perception, the quality of the information they hold is adjudged by the services they offer to the intellectual community. The primary objective of every academic library is to provide relevant materials that will satisfy the needs of its patrons thus, providing information resources to support the aims and objectives of the parent institution through selection, acquisition, organization, and storage of materials demanded by the users.

It is imperative to know that university community of users' needs to be compliant with the university's information security policy, the university's own information security policies must be adhered to at all times when handling university information and the university must ensure it is acting legally when operating such policies. All staff, students and other persons who may handle university information must be made aware of the university's information security policies and of any amendments made to them. Individuals must also confirm that they have read and understood these policies and how they apply to the information they handle (University of Bristol, 2019).For instance, in a study carried out by Sola, et al (2015) revealed that awareness and compliance with library rules and regulations by undergraduate students in two university libraries in Southwest Nigeria revealed that out of 82 respondents, 57(69.5%) indicated that they know about library rules and regulations through library orientation, 6(7.3%) hinted through colleagues, 31(37.8%) reported that through regular visit to the library, while 11(13.4%) expressed that through the library staff. Although, academic libraries are non -profit entity, yet, they still need to make their clients aware of the types of services they provide as well as policies and rules governing the use of their products in the learning community through library orientations, seminars and user education for both old and new students.

For the 21st century the best practices have been the basis for evaluating architectural infrastructural facilities put in place for upgrading the purpose of meeting up with obtains in other climes. Through information and communication technology libraries have been able to re-define library practices with up-to-date ICT facilities that will enhance service delivery beyond their own traditional or manual approach that are becoming so obsolete. To guide against some of these enhancing equipment there is need to provide adequate

security to protect them most of them are not easy to come by in terms of costing and subscription of journals and databases that forms 70% of information resources couple with books and non-book materials. In advanced countries every facet of their services are computerized and well protected thus the need to look at their best practices and localized them by producing some of them through technological transfer. In developing countries most of their security measures heavily rely in policy documents both written and unwritten with adequate orientation, user education couple with application of such policy in every facets of the library departments.

Knowing that it is the role of the librarian to manage the information resources available in the library, as well as to solve the problems of its information unit, thus librarians must be attentive to the new demands and prepared to handle the risk management in information security, going beyond the concern with maintaining computers. In fact, it is also the role of the library to monitor the proper functioning of its equipment and, if necessary, to pass on the demands to the relevant sector, but this alone does not constitute information security, although it is an integral part of a series of actions and best practices. Best practices are the best ways to perform a process, a function, or an activity that leads to a superior performance. These pertaining to the processes, practices, and systems identified in public and private organizations that perform exceptionally well and are widely recognized as improving organization's performance and efficiency. Successfully identifying and applying best practices can reduce costs and improve quality. Best Practices are the means by which leading organizations in any field have achieved top performance, and they serve as goals for the other organizations striving for excellence.

Australian Best Practice Demonstration Program defines best practice as, "the pursuit of world class performance. It is the way in which the most successful organizations manage and organize their operations. It is a moving target. As the leading organizations continue to improve the 'best practice', goalposts are constantly moving. The concept of continuous improvement is integral to the achievement of best practice" Best Practice is a management idea which asserts that there is a technique, method, process, activity, incentive or reward that is more effective at delivering a particular outcome than any other technique, method, and process. Information security is not only Information Technology, as it involves legislation, technical standards, business and technology, and all these factors must be taken into account in the elaboration of an Information Security Policy. In view of this, Vieira (2014) prepared a compilation of the specific legislation related to information security (updated until August, 14, 2014), which includes: Legal Devices of Federal Character; Specific Legislation of Federal Character; State / District Specific Legislation; Specific Legislation of Municipal Character; Technical Standards; Projects of Laws (Vieira, 2014). The management of information security and its implementation in organizations must also be carried out in accordance with the norms of the Brazilian Association of Technical Norms, specifically the "27000 family", and among others related.

In addition, it is important to have a sense of the subject and related issues, such as: errors inherent in the use and manipulation of data (e.g. an email forwarded to the wrong recipient); Network attacks and data theft, counterfeits etc.; Actions of nature (earthquakes,

storms, floods, among others) that could compromise physical structures, including those that safeguard backup data; Financial losses, legal proceedings, fines or contractual penalties; Damage to the image; And on key pests and cyber threats that leave IT resources vulnerable to attack, theft, and data manipulation (Lima, et al 2014). It therefore means that academic libraries should have as one of their priorities the implementation and inclusion of guidelines documented in an Information Security Policy, in order to comply with the International Information Security Standards, and that at the same time, contemplate the particularities and needs of an academic research environment, respecting, of course, the rights and freedom of users, as well as respecting the reality of each library, as well as meeting the Institutional Development of the Institution of Higher Education to which it belongs.

Training is synonymous with drilling, keeping fit on the job, it might take the form of attending conference, seminars, in-house training further studies etc, and the essence is to be exposed to latest development in your profession of librarianship. Suffice to say that Information Security awareness initiatives are seen as critical to any information security programme. But, how do we determine the effectiveness of these awareness initiatives? We could get our employees to write a test afterwards to determine how well they understand the policies, but this does not show how it affects the employee's on the job behaviour. Since awareness training have a direct influence on the security behaviour of individuals, it is necessary that they benefit direct from awareness training (Stephanon & Dagada, n.d.). Every facet of information security in academic library requires training and thus this training add more to existing knowledge which may be tacit or explicit but all are useful in the development of information security in which the bottom line is provision of essential services for users. Nonaka and Takeuchi (1995) argue that there are two types of knowledge and both are needed to help explain organisational learning, i.e. tacit knowledge and explicit knowledge. They propose that an organisation learns by oscillating between the two types of knowledge while tacit knowledge is not tangible and is subjective since it is that which is possessed by employees of the organisation.

This includes individual beliefs, experiences and understandings of the organisation and what the organisation requires from them. Explicit knowledge on the other hand is codified, formal and easily expressed. Examples of this are organisational policies and pamphlets. Nonaka and Takeuchi (1995:70, 71) argue that the learning path in an organisation follows four cyclical stages: a) Employees share tacit knowledge; b) Tacit knowledge is made explicit by formalizing it (e.g. policies); c) Formalized knowledge is disseminated (e.g. awareness activities) and, d) Employees "learn by doing" and thus explicit knowledge is made tacit by employees internalizing it. Where these types of knowledge exist and thoroughly practice in an organisation such as academic institution environment there would be less fear of impacting it on majour stake holders in the academic libraries. It is important to emphasis such training on the information users behavior through compliance and for information security awareness in academic libraries.

Enforcement of security awareness and compliance by information users in academic libraries by librarians has it is own challenges as practitioners on the field. In a previous

study according to Bulgurcu *et al.* cited in Alotaibi, et al (2016)have highlighted the impact of security awareness on employees' behavior awareness has a significant influence on an employee's intention to comply. Puhankinen (2010) carried out action research to validate a training programme on information security policy compliance. The results of the study suggested that increased awareness and training programmes have an impact on users' compliance with information security policy. Chan and Mubarak (2012) concluded that a "lack of awareness and knowledge of policies may have allowed for staff to violate such policies" (p.52).

Most of the challenges of information security awareness in our libraries have to do with funding, such that academic library budget is not enough to provide up-to-date equipment necessary to cater for library an information resources provision and where it has been provided at the inception that there is lack of maintenance. Researchers have addressed the challenges associated with information security policy. Organisations such as academic libraries encounter challenges associated with the promotion and dissemination of their information security policies, while non-compliance with information security policy is considered to be primarily a human problem rather than a technical issue. Researchers have mentioned three types of non-compliance behaviour: such as malicious, negligent and unawareness respectively. The main motivation for malicious behaviour is malicious intent to bring harm to an organisation's information assets and this very common among students who accounted for larger percentages of information users (Furnell & Thomson, 2009).

Many libraries do not continuously review and update their information security policy. Colwill (2009) states that "security policy, controls, guidelines and training are lagging behind changes" (p. 26). Moreover, designing and managing a security policy that meets all the important criteria can be a challenge for many libraries (Silowash, et al 2012). Furthermore, many academic libraries do not update their policy to be more in line with rapidly and constantly developing technology. And, lastly shadow security, there are two types of user behaviour associated with information security policy the need for compliance and non-compliance. However, Kirlappos, et al (2015) have suggested a third type of user behaviour, which is shadow security. Shadow security is defined as "employees going around IT to get the IT services they want on their own" Kirlappos et al (2014). Such employees implement their own security solutions when they believe that compliance is beyond their capacity or will affect their productivity.

CONCLUSION AND RECOMMENDATIONS

The focus of this chapter has been to discuss issues associated with information security awareness policy on compliant behavior of information users in academic libraries and particularly compliant behavior of information users, all personnel which are majorly the librarians, library officers and library management should be able to understand the information security policies of their employers. All information users including university community, students and researchers need to be consistently given awareness training and education on the implemented security policy, without such training and education, the security will have no impact on the employees. It is equally important that compliance with

security is enforced. Doing this will keep the employees abreast of the need to be updated on the policy, technology should play a major role in compelling employees to adhere to the security policy of the library. Moreover, need to continuously subjecting information users to targeted awareness rising and dynamically monitoring their adherence to information security policy should increase their compliance level.

REFERENCES

Alotaibi, M., Furnell, S., & Clarke, N. (2016). *Information security policies: A review of challenges and influencing factors.* Security Research Institute, Edith Cowan University, Perth, Western Australia Centre for Research in Information and Cyber Security, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa.

Aloul, F. A. (2012). The need for effective information security awareness. *Journal of Advances in Information Technology, 3*(3), 45-65.

Ameyaw, S. (2018). Compliance to library rules and regulations by students: a case study of Walton Whaley Library of Valley View University. *Library Philosophy and Practice,*2203.

Boyce, J.,& Jennings, D. (2002). *Information assurance: Managing organizational IT security.* Butterment Heinemann. 216p.

Chan, H.,& Mubarak, S. (2012). Significance of information security awareness in the higher education sector. *International Journal of Computer Applied,60*(10), 23–31.

ENISA (2006). *A new users' guide: How to raise information security awareness.* 2008 European Network and Information Security Agency.

Furnell, S., & Thomson, K. L. (2009). From culture to disobedience: Recognizing the varying user acceptance of IT security. *Computer Fraud Security, 9*(2), 5–10.

Hansche, S. (2001). Designing a security awareness program: Part 1.*Information Systems Security,9* (6), 1-9.

John, N. (1998). Libraries and the global information infrastructure. Retrieved from: www.unesco.org/webworld/infoethics2/eng/papers/paper _13.rtf

Kamal, S., Zaini, M. K., Zulhemay, M., Shahibi, M. S., & Ali, J. (2012). Information security awareness amongst academic librarians. *Journal of Applied Sciences Research, 8*(3), 30-45.

Kirlappos, I., Parkin, S., & Sasse, M. A. (2015). Shadow security as a tool for the learning organization, 45, (1). 29-37.

Lima, J. S., Araujo, A. R. S., Santos, F. E. P., Barbosa, L. G., & Santos, I. L., (2014). Digital Biblioteconomiae Ciência da Informação RDBCI: *Digital Journal of Library and Information Science.*

Ma Jun-tao, D., Huang, Q., & Wen, S. X. (2010). Network Security risks in digital medical libraries and their preventive measures. *Chinese Journal of Medical Library and Information Science,19*(6), 60-1.

Maidabino, A. A., & Zainab, A. N. (2011). Collection security management at university libraries: Assessment of its implementation status. *Malaysian Journal of Library and Information Science,16*(1), 15-33.

Ogunsola, L. A. (2011). The next step in librarianship: Is the traditional library dead? *Library Philosophy and Practice*. https://digitalcommons.unl.edu/libphilprac/2124.

Ossai-Ugbah, N. B. (2013). The role of the library and librarians in promoting national security in Nigeria. *Academic Journal of Interdisciplinary Studies*, 2(2).

Puhakainen, P., & Siponen, M. (2010). Research article improving employees through information systems. *Security Training*, 34(4), 757–778.

Ramos, M. M. (2007). The role of librarians in the 21st Century. Paper delivered during the 35th ALAP Anniversary Forum. http://www.slideshare.net/plaistrlc/

Silowash, G. D., Cappelli, D., & Moore, A., (2012). *Common sense guide to mitigating insider threats*. 4th Edition.

Sola, E. O., Oluwafemi, A. I., & Bukola, D.A. (2015). Awareness and compliance to library South-west Nigeria. *International Journal of Library Science*, 4(1), 1-6.

Stephanon, A. T., & Dagada, R. (n.d). The impact of information security awareness training on information security behaviour: The case for further research. University of the Witwatersrand.

Unegbu, C. P., Ugah, A. D. Nwosu, M. C., & Aniedu, O. N. (2013). Increasing clients' use of electronic resources in academic libraries: a practical service strategy. In: Issa, A.O., Igwe, K. N.& Uzuegbu, C.P. (Eds). *Provision of Library and Information Services to Users in the Era of Globalisation*. Lagos: Waltodammy Visual Concept.

University of Bristol (2019). Information security of policy-compliance policy, Available at: http://www.bristol.ac.uk/media-library/sites/infosec/documents/ISP-03%20v1.2.pdf

Uzuegbu, C. P., & Caroline, A. O. (2013). Security practices in Nigerian university libraries. *PNLA Quarterly*,77(2), 18-27.

Vieira, T. M. (2014).Compilação de Legislação específica relacionada à segurança da informação (atualizada até 14 de agosto de 2014).

Von, S. B. (2000). Information security- the third wave? *Computers and Security*, *19*, 615-620.