AFRICAN MULTIDISCIPLINARY JOURNAL OF DEVELOPMENT

AN EVALUATION OF THE IMPLEMENTATION OF INFORMATION COMMUNICATION TECHNOLOGY PROCEDURES IN ASSURING THE INFORMATION SECURITY STANDARDS IN COLLEGES OF EDUCATION IN NIGERIA

Salami Afolabi Kehinde

School of Computing and Information Technology,
Kampala International University, Kampala, Uganda

ABSTRACT

The study assessed the implementation, enforcement and compliance of Information Communication Technology (ICT) policies in assuring the information security standards in thirteen Colleges of Education who's their selection was based on geo political zones of Federal Republic of Nigeria. The study employed cross sectional survey design where the population considered was 1,593 and only took a sample of 118 and data was collected using questionnaires, interviews and documentary reviews. The study found that ICT policy implementation and information security mechanisms were still at basic though in most instances where satisfactorily implemented. Further revealed that the changing nature of knowledge and changing capabilities of technology require colleges of education to implement ICT in their teaching roles to enable the high levels of know-how and develop the skills of ICT innovations in colleges of Education. Therefore, it can be concluded that good implementation of ICT policies is a prerequisite for high level performance of information security. The study recommended an in-depth detailed comprehensive implementation of the following ICT policies in order to ensure information security in terms of confidentiality, integrity and availability, access control mechanisms, terms and conditions of ICT usage, backup and recovery mechanism and disaster recovery mechanisms.

Keywords: ***ICT Policies, Education, Security, Enforcement and Compliance, ICT Implementation and Information Security, Technology Deployment***

INTRODUCTION

The Education system is one the sectors that Information and Communication Technology (ICT) policy initiatives in Nigeria have been targeting since 1988 (Adebowale & Dare; Yusuf, 2005, 2007). However, three decades since then, little impact of ICT has been felt in this sector more especially in the Colleges of Education (Garba, Singh, Yusuf, & Ziden, 2013; Tella, 2011; Yushau & Nannim, 2018). This study examines the relevance of ICT policy implementation with a focus on the information security in Colleges of Education in Nigeria.

The rest of the paper is organized as follows; the next section gives the background of the study. A detailed literature review on the subject understudy is presented. Thereafter the background of study is followed by the theoretical framework of the study that gives the underpinning theories on which this study is based. The methodology follows theoretical framework and it gives the methods used to capture data for this study. The methodology is followed by the findings that present the major findings revealed about the colleges of education. Finally, we present the discussion and recommendations and conclusions in the last section of the study.

The International Standards such as ISO 27002 are good starting point to implement ICT Security in any national system (Diver, 2007; Flowerday & Tuyikeze, 2016; Hong, Chi, Chao, & Tang, 2006; Hong, Chi, Chao, & Tang, 2003; Tuyikeze & Flowerday, 2014). In addition, (Bayuk, 2009) support the idea of using international standard as baseline framework because they increase trust in the organization. He stated that this is a reasonable approach as it helps to ensure that the policy will be accepted as adequate not only by higher education management but also by external auditors and others who may have stake in the organization security programme.

The main reason to develop ICT security implementation policy is to mitigate the various security risks that organization face (Tuyikeze & Flowerday, 2014). However, the process of developing the policy requires the organization first to identify and understand regulatory requirements that dictate creation of such policies before writing information security policy. (Avolio & Fallin, 2007) suggest that information security policy developers must familiarize themselves with penalties of non- compliance with laws. Therefore, it is necessary that colleges obtain legal advice that the policies are binding. Successful implementation of ICT security policies requires security awareness at all levels of the organization. ICT security awareness should be created through widely disseminated documentation, newsletter, emails a website, training programs and other notifications about security issues.

For ICT security implementation goals to be realized, users of IT resources should be trained to make them to be aware of potential security concern and understand their responsibility to report security incident and vulnerabilities.

(Okesola, Onashoga, & Ogunbanwo, 2016) observed that in Nigeria Information and Communication Technology (ICT) was introduced into Nigeria Education System curriculum in 2000. Prior to 1988 a lot of policy initiatives were developed to bring ICT security implementation into reality; this led to producing a National ICT Policy draft in January 2012. In Nigeria colleges the Chief Information Security Officer (CISO) is charged with the responsibility of implementing the ICT security and must ensure compliance where there are lapses disciplinary actions must be taken to sanction any criminality. Therefore, the CISO must work with the overall head of the organization. In Nigeria collages efforts are been made to develop security policies

program to address the overall ICT security implementation and IT security goals which apply to all IT resources within the institution. Program policies usually address confidentiality or service availability. Therefore, all program policies must meet and follow, comply with existing laws, regulations of state and federal policies.

Users at all levels should be trained in appropriate use of technology and developing appropriate user policies and enforcement of those policies. In as much as the Nigeria colleges of education have tried to ensure good ICT security implementation there are noticeable challenges such as vandalisation of ICT equipment, Slow internet, Erratic power supply, users do not familiarize themselves with ICT security policies and problem of sustainable maintenance of ICT equipment just to mention a few.

LITERATURE REVIEW

According to (Kearney & Kruger, 2013; Kruger & Kearney, 2008) ICT resources are important assets of any organization. Protection of these resources is equally important. To be able to protect themselves and their profitability many organizations have established information security awareness programs. In order for a security awareness program to add value to an organization and at the same time make a contribution to the field of information security it is necessary to have a set of methods to study and measure its effects.

One of the key defences to address human oriented controls is the implementation of an information security awareness program. These programs are used to create and maintain security positive behaviour amongst employees and the goal of such programs would be to highlight the importance of information security systems and possible negative effects of security breach or failure. The importance of security awareness program is further emphasized in the BS7799:1 where the objective of user training is given as to measure that all users are aware of information security treats and concerns.

Following the implementation of information security awareness program there is usually a normal business need to evaluate and measure the success and effectiveness of it. (Schlienger & Teufel, 2002) stated that evaluation should always be the final step in an information security management program in order to obtain information on efficiency and effectiveness of actions to define follow up actions and to justify investments in the program.

Theoretical framework for this study

We based our study on existing well know theoretical frameworks in the domain of information security (Bell, 2006; McClelland, 2010).

The Protective Security Policy Framework (PSPF) (McClelland, 2010) highly put in practice by the Australian Government is committed to effectively managing the protective security risks to Government business and building interest trust confidence and engagement with the Australian people and their international partners. The Government requires agency heads to have in place effective protective security arrangement to ensure that respective agency's capacity to function, the safety of those employed, the function of government and those who are clients of government and official resources and information the agency holds in trust both from and for the public and those provided in confidence by other counties, agencies and organisations are safeguard.

To achieve this, agencies are to apply the protective security policy framework and promote protective security as part of their agency's culture.

The Bell-La Padula (BLP) model (Bell, 2006) is a model of computer security that focuses on mandatory and discretionary access control. A mandatory access control scheme is where one trusts user/process (usually the system administrator or perhaps the operating system itself) creates and enforces the rules for access control. A discretionary access control scheme is one where the owner of a file can manipulate the access control permissions to their desire.

The first goal of the Bell-La Padula security model is to prevent users from gaining access to information above their security clearance. In other words, a user with "Classified" access (a low-level clearance) should not be able to read files marked as "Top Secret" (a higher level of secrecy), but someone with "Top Secret Access" should. The model calls this the Simple Security Property, because a naiive security model might consider this sufficient. The way that the security model deals with this problem is through an Access Control List. Every file had an associated structure (called an Access Control List) that lists the permissions of every user in regards to the file. The language of the original model: "The Access Control List in Multics is a list of "(process, ring bracket)" pairs (for our purposes here, the Multics analogue of subjects) allow access to a segment (that is, an object) and the modes of access allowed."

The second goal is the protection of information containers rather than of the information itself. That is, a malicious program might pass classified information along by putting it into an information container labelled at a lower level than the information itself. In other words, there's nothing in the Simple Security Property to stop a malicious Top-Secret level user from reading information in one file, then copying that information into a new file which is able to be read by a user with a lower-level security clearance. To combat this flaw, Bell & La Padula came up with the "property", which is described as "a subject at a given security level must not write to any object at a lower security level." In other words, you can only create documents of an equal or higher level security than your access level. This property is called "write up".

METHODOLOGY

Based on the above discussed theoretical background, the study adopted a cross sectional survey design. This is a design where by data is collected at one point in time from the cross sectional of the study population (Creswell, 2012). In addition, the study employed both quantitative and qualitative approaches (Creswell, 2011). The choice for this approach was based on the premise that when quantitative and qualitative methods are used in combination a more complete analysis would be obtained since they complement each other (Morse, 2003). Quantitative approach depends upon the collection of quantitative data such as statistics and percentages. This approach uses a number of methods and models such as time-series analysis and input-output analysis, and often it contains descriptive statistics and inferential statistics in order to test the raw data and to unveil the facts accordingly. In other words, it is the process of presenting and interpreting numerical data. The objective of quantitative research in this study was to employ theories, and hypotheses pertaining to the phenomena under research. Quantitative method is widely used in social sciences such as economics, marketing, and political science hence it was deemed relevant in this study (Bryman, 2006).

On the other hand, the qualitative approach is based upon developing a hypothesis, for example, based upon the actual scenario in the education sector. The qualitative approach relies primarily on the collection of qualitative data in form of words, pictures, and objects. This method is employed in many different academic disciplines and traditional social sciences. The qualitative approach introduces information only on particular hypotheses and Quantitative methods can be used to verify which of such hypotheses are true (Lazo, 2010).

Additionally, it aims to gather in-depth understanding of human behaviour which involves extensive study of the claims made by the researcher according to the previously conducted work.

Study Population

In this research, the study population included the entire staff (both teaching and non-teaching staff) of the colleges of education in Nigeria, 1,593 in total. The target population refers to the total number of subjects or the total environment of interest to the researcher (Onen, 2016). The target population of this study included only the staff members who worked in the ICT departments of the colleges of education on Nigeria. This was considered due to the nature of the research. They were 170 in total and they included system administrators, ICT support technicians, ICT laboratory assistants and ICT support staff. Head of departments should be able to, oversee the activities of the departments. The Head of department plays a key and vital role in the scheme of things. Therefore, system administrators must be supportive and give Head of department full cooperation as they must work together as partners in progress to move the organization forward.

This study involved systems administrators because they are charged with the role of installing, supporting and maintaining servers or other computer systems, and planning for and responding to service outages and other ICT problems within the college. Furthermore, ICT support technicians were involved in this study because they provide technical support and assistance for users of computer infrastructure and web technologies. They also undertake diagnosis and resolution of technical problems. Table 3.1 gives the summary of the target population.

Similarly, this study included the laboratory assistants because they coordinate scheduling of students and lecturers for the purpose of maintaining computer lab operations and activities, and instructing students and lecturers in computer lab technology and software applications. Lastly, ICT support staff were included in the study because they deal with the day to day issues of maintaining a trouble-free environment for effective use of ICT equipment, assisting staff and students to overcome any difficulties they may be experiencing e.g. printer failure, poor PC performance, etc., and performing daily checks on all ICT equipment to ensure it is inacceptable working order. The researcher used both simple random sampling (probability sampling) and purposive sampling (non-probability sampling) to select the above respondents.

Sample Size

Sample size refers to the number of individual pieces of data collected in a survey. Sample size measures the number of individual samples measured or observation used in a survey. A sample size is part of the target or accessible population that the researcher has chosen to study, representing the rest of the other members of the population (Creswell, 2012). The sample size of this study remained 118 respondents (*refer* to table 3.1).

Table 3. 1 Sample of the Target Population

Colleges of Education in Nigeria	Target Population			
	Systems Administrator	ICT Technicians	ICT Laboratory Assistants	ICT Support Staff
Federal College of Education, Zaria	1	2	1	6
Federal College of education (T), Bichi	1	3	3	3
Federal College of Education (T), Gusau.	1	2	3	8
Federal College of Education, Kano.	1	3	4	4
College of Education, Oyo (special)	1	2	2	3
Federal College of Education, Yola	1	1	3	4
Lagos State College of Education, Ijanikin	1	2	3	7
Federal College of Education, Okene	1	2	1	5
College of Education, Yenagoa	1	2	3	6
Federal College of Education, Omoku	1	2	2	4
FCT Zuba College of Education, Abuja	1	2	2	7
Sub total	**11**	**23**	**27**	**57**
Overall Total	**118**			

Sampling Technique

According to (Johnson & Christensen, 2014), having established the actual sample size required, the researcher needs to select the most appropriate sampling technique to obtain a representative sample. Sampling technique basically refers to the method employed in obtaining the sample size for the research. According to (Mugenda & Mugenda, 2003) sampling technique is very necessary in any social study because it helps in answering questions pertaining to what type of respondents were called upon to give answers to the research questions,

whether the selected group of respondents is adequately representative of the population, how wide a coverage would be acceptable and other questions that would help the researcher in the selection of his sampling design.

According to (Saunders, Lewis, & Thornhill, 2007), five main techniques can be used to select a probability sample: simple random; systematic; stratified random; cluster; and multi-stage. Simple random sampling involves selecting the sample at random from the sampling frame using random number tables, a computer or an online random number generator, such as Research Randomizer (2008). In this study, the researcher used online random number table to select the following category of respondents: ICT technicians, ICT laboratory assistants, and ICT support staff.

This study also employed non-probability sampling, that is, purposive sampling technique, first to select the Colleges of Education in the different States that make up northwest geopolitical in Nigeria. Secondly, the study used purposive sampling to select the ICT team from each of the selected Colleges of Education given their already small number. The method was used because it enabled the researcher to identify uniquely qualified respondents to provide needed information. The selection was based on expert knowledge of the particular problem of the research. This helped the researcher to select respondents who seemed to know more and work directly with the implementation of ICT policies and information security.

Data Source

This study included both the primary and secondary sources of data collection. The primary source refers to the data collected using questionnaires and interviews while the secondary data was collected using documentary analysis from books, articles, journals, published thesis/dissertations, government reports on ICT policies, ICT policy of every College under study, and their different information security mechanisms such as data integrity, authentication of users, identification & authentication of users.

Data Collection Methods

The study adopted three methods of data collection, namely: questionnaire survey, interview survey and document analysis.

The questionnaire survey was done objective by objective targeting the system administrators, ICT support technicians, ICT laboratory assistants and ICT support staff to respond to questions regarding ICT policy implementation and information security. The data collection tool employed in this method was questionnaires (structured questionnaire). The questionnaire was preferred because it is easy to administer, saves time and allows for doubts to be clarified on spot from many respondents (U. Sekaran, 2003).

The interview survey method was used to collect data from at least the systems administrators from each of the Colleges under survey. This method was helpful in collecting data regarding ICT policies. The researcher preferred this method because it enables the researcher to probe more and even read actions and expressions of the key informants (Jackson, 2009).

The documentary analysis method was used to obtain information related to the study from a variety of written materials from scholars, and authors. Specifically, the researcher analysed ICT policies in each of the colleges and their information security mechanisms using a documentary

checklist. This method was helpful to the researcher to establish facts, current trends, relationships, critics, gaps, and how the study would cover the gaps in addressing ICT policy implementation and its effectiveness in ensuring information security (Freebody, 2003)

Pilot Study

Before the actual survey, pilot study was conducted with a sample of 20 respondents from one of the colleges in northwest Nigeria similar to the final population in the sample to refine the questionnaire, identify any loopholes in the questionnaire and anticipate any logistical problems during the actual survey. Respondents were asked to point out any part of the questionnaire they found to be unclear or complicated. The pilot study was conducted to gather any additional information about ICT policy implementation and information security from the respondents that could help to further refine the research and address issues that may have been left out. Indeed, a number of irregularities were found in the questionnaire. For example, some questions were cited to ambiguous, meaningless, and unclear. The researcher therefore adjusted them accordingly. The researcher refined the questions using the simplest possible language which even non-ICT personnel would understand.

Validity and Reliability

The validity of a value is a descriptive term used to indicate how accurately the recorded values reflect the concept being measured. (Burns, 2018) describes five types of validity, which include predictive, concurrent, content, construct and face validity. From a research point of view, construct validity is generally considered most important, and is the type of validity that was employed in this study. Construct validity refers to the degree to which inferences can legitimately be made from the measures being studied to the theoretical constructs on which those measures are based (Trochim, 2007). A factor analytic technique was widely used to assess the construct validity of a measure. The technique examines whether items considered to represent a particular construct have a stronger or preferred factor loading on one construct compared to all others (Stevens, 2009).

In this study, all items representing one or more of the research constructs was subjected to exploratory factor analysis (EFA) using principal component analysis with varimax rotation. In identifying the factors, four commonly employed rules were followed: a) retain only factors whose Eigen values were greater than 1.0; b) retain only items with a minimum factor loading of 0.50; c) remove items with loadings above 0.50 on two or more factors; and d) remove factors with only one item (Burns, 2018).

Reliability refers to the consistency, stability over time, and dependability of the values (Burns, 2018), or in other words, how free they are from random error. Although there are four commonly used methods for computing reliability estimates, which include test-retest, alternate forms, split-half, and internal-consistency; the study employed internal consistency which indicates the reliability to which the constituent items all measure the same underlying attribute. In developing the internal-consistency method, (ATSB, 2013) formulated measures of reliability that used item statistics as the basic unit of measurement. A frequently used statistic, and the one that was adopted in this study, was the Cronbach alpha coefficient. Reliability was determined through the interpretation of Cronbach's alpha, which is a reliability coefficient that indicates how well the items in a set are positively correlated to one another (Hee, 2014; Uma Sekaran & Bougie, 2016). The reliability of each measure was assessed by coefficient alpha using statistical package for social sciences (SPSS) version 22.

The Findings

This describes the analysis of data followed by a discussion of the research findings. The findings relate to the research objectives that guided the study. Data was analysed to identify, describe and explore the relationship between ICT policy implementation and information security of Colleges of Education in Nigeria. The researcher used five Likert scale but with five levels in the tables, only three values were used because the respondents did not use the rest.

Description of the respondents in the study: Demographic characteristics of the respondents

A descriptive summary of the 114 study participants has been presented in Table 4.1 below. Majority of the respondents were males (68.42%) and aged 20-29 years (51.75%). The highest proportion of respondents had attained Diploma level (45.61%) education and had 1 to 5 years (50%) experience in ICT information security. The highest proportion of respondents was ICT support staff (36.84%). Majority of the respondents had no special training in ICT information security (78.95%).

Access Control Mechanisms

Respondents were asked to provide feedback on the extent to which the respective Colleges of Education they work for have access control mechanisms. As to whether all College staff had access to computers, majority of the respondents strongly agreed (92.11%) while the minority agreed (7.02%) and strongly disagreed (0.88%). As to whether usernames and passwords were changed periodically, majority of the college ICT staff agreed (67.54%), followed by those who strongly agreed (26.32%) and only a few reporting not to be sure (4.39%) and disagreeing (1.75%). As regards all non-system administrator staff having limited access to ICT information from any computer, majority of the respondents strongly agreed (55.26%), followed by those who agreed (39.47%) and lastly those who weren't sure (5.26%).

Table 4. 1 Characteristics of Respondents

Variable	Frequency	Percent
Sex		
Male	78	68.42
Female	36	31.58
Age		
20-29 years	59	51.75
30-39 years	38	33.33
40-49 years	14	12.28
Above 50 years	3	2.63
Education level		
Certificate	38	33.33
Diploma	52	45.61
Bachelor degree	20	17.54
Master Degree	3	2.63
PhD	1	0.88

Variable	Frequency	Percent
ICT training Information Security		
Yes	24	21.05
No	90	78.95
Experience in ICT		
Less than 1 year	38	33.33
1-5 years	57	50.00
6-10 years	15	13.16
More than 10 years	4	3.51
Position		
Systems Administrator	7	6.14
IT Technician	32	28.07
ICT support staff	42	36.84
Others, Specify	33	28.95

Table 4. 2 Access Control Mechanism (ACM)

Variable	Strongly Disagree		Disagree		Not sure		Agree		Strongly agree	
	freq.	%	freq.	%	freq.	%	freq.	%	freq.	%
ACM1	1	0.88					8	7.02	105	92.11
ACM2			2	1.75	5	4.39	77	67.54	30	26.32
ACM3					6	5.26	45	39.47	63	55.26

Terms and Conditions of ICT Usage

Respondents interviewed concerning terms and conditions of ICT usage in the respective Colleges of Education were 105. This too is one of the key components of ICT policy implementation. Pertaining to having a provision for all staff to sign an agreement on terms and conditions of using ICT facilities, only half of the respondents strongly agreed (50%) while the rest just agreeing (46.69%) and the least weren't sure (3.51%). As regards only employed staff having access to ICT facilities, the highest proportion strongly agreed (48.25%) and agreed (43.86%) with on 7.89% reporting not to be sure. As to whether all terminated staff must return all ICT facilities in their possession to the College management, majority strongly agreed (64.91%) followed by those who agreed (28.95%) and lastly those who weren't sure (6.14%). Regarding the College reserving the right without notice to limit or restrict any individual's use and to inspect, copy, remove or otherwise alter data, files or system resource which is used in violation of College rules or policies is summarized in Table 3 below as well. Majority of respondents strongly agreed (65.79%) while the rest either agreed (32.46%) or weren't sure (1.75%).

Table 4. 3 Terms and conditions of ICT usage (TCU)

Variable	Strongly Disagree		Disagree		Not sure		Agree		Strongly agree	
	freq.	%	freq.	%	freq.	%	freq.	%	freq.	%
TCU1					4	3.51	53	46.49	57	50.00
TCU2					9	7.89	50	43.86	55	48.25
TCU3					7	6.14	33	28.95	74	64.91
TCU5					2	1.75	37	32.46	75	65.79

Backup and Recovery Mechanism

This is also a key component of ICT policy implementation and so respondents were asked how their respective Colleges of Education fared on some aspects of the component as summarized in Table 4. As regards to whether backups are scheduled to run after working hours, majority of the respondents agreed (51.75%) followed by those who strongly agreed (45.61%) and lastly those who weren't sure (2.63%). As to whether there are daily, weekly and monthly backups in their Colleges of Education, majority of the respondents strongly agreed (63.16%) with the rest agreeing (34.21%) or reporting that they weren't sure (2.63%). Regarding whether backup procedures are documented in writing and updated on a regular basis as changes are required, the highest proportion of respondents strongly agreed (52.63%) and agreed (43.86%) with on 3.51% reporting not to be sure. Concerning their being a system administrator assigned to perform system backups, the highest proportion of respondents strongly agreed (57.02%) followed by those who agreed (39.47%) and lastly those who weren't sure (3.51%). Pertaining to whether access to backup copies in a safe or storage area is limited to the system administrators doing the backups, majority of the respondents strongly agreed (53.51%), followed by those who agreed (42.98%), then those who weren't sure (2.63%) and lastly those who disagreed (0.88%). With regards to whether in order to recover data, a detailed assessment of extent of damage to network infrastructure in the server room is done, majority of the respondents strongly agreed (77.19%) with the rest agreeing (22.81%). As to whether if information systems are affected, relevant backup media are located and validated, the highest proportion of respondents either agreed (51.75%) or strongly agreed (42.98%) while the rest weren't sure (5.26%). Pertaining to whether external expertise is sought in order to recover critical data, the highest proportion of respondents strongly agreed (40.35%) and agreed (40.35%) followed by those who weren't sure (16.67%), then those who disagreed (1.75%) and lastly those who strongly disagreed (0.88%).

Table 4. 4 Backup and recovery mechanism (BRM)

Variable	Strongly disagree		Disagree		Not sure		Agree		Strongly agree	
	freq.	%	freq.	%	freq.	%	freq.	%	freq.	%
BRM1					3	2.63	59	51.75	52	45.61
BRM2					3	2.63	39	34.21	72	63.16
BRM4					4	3.51	50	43.86	60	52.63
BRM5					4	3.51	45	39.47	65	57.02
BRM6			1	0.88	3	2.63	49	42.98	61	53.51
BRM8							26	22.81	88	77.19
BRM9					6	5.26	59	51.75	49	42.98
BRM10	1	0.88	2	1.75	19	16.67	46	40.35	46	40.35

Disaster Recovery Plans and Mechanisms

Table 4.5 provides a summary of respondent's feedback when asked about disaster recovery plans and mechanisms in their Colleges of Education. When asked whether the turnaround time to receive a backup tape for recovery was a maximum of two hours, the highest proportion strongly agreed (51.75%) and agreed (4.86%) though 4.39% were not sure. As regards backup information being given an appropriate level of physical and environmental protection consistent with standards applied at the main site, majority of the respondents strongly agreed (62.28%) followed by those who agreed (31.58%) and lastly those who were not sure (6.14%). Concerning whether backup media is regularly tested, where applicable to ensure that they can be relied upon for emergency use when necessary, the highest proportion of respondents strongly agreed (54.39%) and agreed (42.11%) with only 3.51% not sure. As regards restoration procedures being regularly checked and tested to ensure that they are effective and that they can be completed within the recovery time that has been allotted in operational procedures for recovery, the highest proportion of respondents strongly agreed (55.26%) and agreed (42.11%) with only 2.63% not sure.

Table 4. 5 Disaster recovery plans and mechanisms (DRP)

Variable	**Strongly disagree**		**Disagree**		**Not sure**		**Agree**		**Strongly agree**	
	freq.	%	freq.	%	freq.	%	freq.	%	freq.	%
DRP2					5	4.39	50	43.86	59	51.75
DRP4					7	6.14	36	31.58	71	62.28
DRP5					4	3.51	48	42.11	62	54.39
DRP6					3	2.63	48	42.11	63	55.26

Information Security

The respondents were asked as series of questions corresponding to specific aspects of information security. A description of how the samples Colleges of Education performed with regards to each of these aspects is provided below based on the responses of ICT personnel interviewed.

Identification and Authentication

This is one of the key aspects of information security. Information on how the colleges of education fared on this is summarized in Table 4.6. Concerning every staff having an independent identification code when accessing information from a computer, majority of the respondents strongly agreed (84.21%) with the minority agreeing (14.91%) as well as not being sure (0.88%). As concerns every staff having a user account, username

and password, majority of the respondents strongly agreed (50%) while the minority either disagreed (0.88%) or weren't sure (0.88%).

Table 4. 6 Identification and Authentication

Variable	Strongly disagree		Disagree		Not sure		Agree		Strongly agree	
	freq.	%	freq.	%	freq.	%	freq.	%	freq.	%
IA1					1	0.88	17	14.91	96	84.21
IA2			1	0.88	1	0.88	55	48.25	57	50.00

Authorization

Different staffs have different access privileges given to them by the system administrator. Majority of the staff strongly agreed (65.79%) with the lowest proportion reporting that they weren't sure (2.63%). Furthermore, with regards to all staff being registered so as to use ICT facilities, majority of the staff strongly agreed (55.26%) while the minority weren't sure (1.75%).

Table 4. 7 Authorization

Variable	Strongly disagree		Disagree		Not sure		Agree		Strongly agree	
	freq.	%	freq.	%	freq.	%	freq.	%	freq.	%
AZ1					3	2.63	36	31.58	75	65.79
AZ2					2	1.75	49	42.98	63	55.26

Confidentiality

Pertaining to information being accessed by authorized personnel only, the highest proportion of respondents agreed (48.25%) closely followed by those who strongly agreed (47.37%) while the minority weren't sure (4.39%). Additionally, concerning data being protected from passive attacks and hackers, majority of the respondents strongly agreed (64.91%), with a lower proportion agreeing (31.58%) and a lesser proportion not sure (3.51%). As to whether data privacy was practiced, majority of the respondents agreed (48.25%), followed by those who strongly agreed (44.74%), then those not sure (6.14%) and lastly those who disagreed (0.88%).

Table 4. 8 Confidentiality

Variable	Strongly disagree		Disagree		Not sure		Agree		Strongly agree	
	freq.	%	freq.	%	freq.	%	freq.	%	freq.	%
CT1					5	4.39	55	48.25	54	47.37
CT2					4	3.51	36	31.58	74	64.91
CT3			1	0.88	7	6.14	55	48.25	51	44.74

Integrity

With regards to data being kept from being changed in unauthorized ways (IT1), majority of the respondents strongly agreed (80.70%) and only a minority either agreed (18.42%) or disagreed (0.88%). As to whether data is ensured to be accurate and in good condition (IT2), the highest proportion of respondents agreed (57.02%), followed by those who strongly agreed (33.33%) then those who weren't sure (9.65%). In addition, with reference to whether the system administrator encrypts vital information for security reasons (IT3), majority of the respondents strongly agreed (64.91%) with the rest either agreeing (28.07%) or not sure (7.02%).

Table 4. 9 Integrity

Variable	Strongly Disagree		Disagree		Not Sure		Agree		Strongly Agree	
	freq.	%	freq.	%	freq.	%	freq.	%	freq.	%
IT1			1	0.88			21	18.42	92	80.70
IT2					11	9.65	65	57.02	38	33.33
IT3					8	7.02	32	28.07	74	64.91

Availability

With regards to information always being available at the time it's needed, the highest proportion of respondents strongly agreed (50.88%) and agreed (46.49%) with only a minority not sure (2.63%). Pertaining to whether the system administrator ensures that the computing systems used to store and process information, the security controls used to protect it, and the communication channels used to access it are functioning correctly, majority of the respondents strongly agreed (64.91%). As concerns the college having very good network security mechanisms to prevent external attacks that might compromise data availability, the highest proportion of respondents strongly agreed (56.14%) and agreed (42.98%).

Table 4. 10 Availability

Variable	Strongly Disagree		Disagree		Not sure		Agree		Strongly Agree	
	freq.	%	freq.	%	freq.	%	freq.	%	freq.	%
AT1					3	2.63	53	46.49	58	50.88
AT2					8	7.02	32	28.07	74	64.91
AT3					1	0.88	49	42.98	64	56.14

ICT Policy Implementation and Information Security

In order to study the association between ICT policy implementation and information security, the feedback of the respondents to respective questions used to evaluate each of the components of both ICT policy implementation and information security were averaged and a new scale generated. This scale ranked the performance of the various colleges of education ranging from being very unsatisfactory to being satisfactory based on self-reported responses of staff from the colleges interviewed. For respondents whose responses when averaged for a specific component of either ICT policy implementation or information security ranged from 1 to 1.8, the college was considered to have very unsatisfactory performance on that component. In detail, the categorizations included; very unsatisfactory (1 to 1.8), unsatisfactory (1.81 to 2.60), fairly

satisfactory (2.61 to 3.40), Satisfactory (3.41 to 4.20) and Very satisfactory (4.21 to 5.00).

Table 4. 11 Association between components of ICT policy implementation and information security

Variables	**Information Security**		
Access Control Mechanism	**Satisfactory**	**Very Satisfactory**	**N**
Fairly satisfactory	0.00	100.00	1
Satisfactory	8.33	91.67	12
Very satisfactory	5.94	94.06	101
Terms and Conditions of ICT usage			
Satisfactory	10.00	90.00	10
Very satisfactory	5.77	94.23	104
Backup and Recovery Mechanism			
Satisfactory	18.18	81.82	11
Very satisfactory	4.85	95.15	103
Disaster Recovery Plans and Mechanisms			
Satisfactory	66.67	33.33	6
Very satisfactory	2.78	97.22	108

Table 4.11 above provides a summary of the association between the components of ICT policy implementation and information security. Concerning access control mechanisms, all colleges of education performed at least fairly satisfactorily. Furthermore, majority of the colleges with a very satisfactory access control mechanism had very satisfactory information security (94.06%). Regarding terms and conditions of ICT usage, majority of colleges with very satisfactory performance had very satisfactory information security (94.23%). Similarly, majority of colleges with very satisfactory backup and recovery mechanisms also had very satisfactory information security (95.15%). Likewise, majority of colleges with very satisfactory disaster recovery plans and mechanisms had very satisfactory information security (97.22%).

Figure 4.1 below provides a summarized description of the performance of colleges of education with regards to information security. 93.86% of the colleges had very satisfactory performance while 6.14% had satisfactory performance.

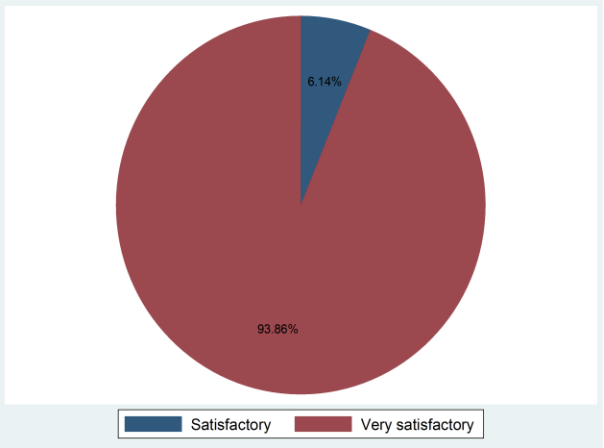

Figure 4.1 Respondent overall rating of Information Security

Information security in the analysis was rated as very satisfactory performance. Every staff should have an independent identification code when accessing information from the computer. Authentication is another great factor for consideration. People can authenticate themselves in three basic ways namely; something they know such as password, something they have such as code or token or card. Fingerprint scans, retina scans, iris scans, finger vein scans, etc.. Other factors must be put in place such as confidentiality integrity availability (CIA).

In conclusion it can be deduced that if all these measures are taken into consideration it will definitely guarantee information security in the colleges.

RESULTS AND DISCUSSION

It was found that ICT policies were satisfactorily implemented in most of the surveyed Colleges of Education. This was attributed to the fact that respondents indicated that variables such as access control mechanism, terms and conditions of ICT usage, backup and recovery mechanism, disaster recovery plans and mechanisms were satisfactorily implemented ICT policies in their colleges.

This finding of the study is consistent with (Peansupap & Walker, 2006) work. There should be an ICT implementation process for providing learning that concurrently integrates both technical and organizational support. The authors further explained learning and training content coupled with delivery quality may be important constraint issues. Basic ICT training can be integrated into ICT policies so that users can be aware of concepts and benefits of technical know-how. Not until

such level of literacy is attained among users, then no high level of ICT innovation in their work processes.

In a related development ICT implementation and adoption is a management intensive activity that managers should reframe. Implementation on expectations create small win and reduce any conflict of interest. However educational policy makers are in unique position to bring about change. This is illustrated in a study of 174 ICT supported innovative classroom in 28 countries (Kozma, 2005). In 127 cases there were explicit connection between the innovation and national policies that promoted the use of ICT (Jones, 2003). But while the introduction of ICT policy is necessary for change. It is not sufficient to result in its implementation or impact (Tyack & Cuban, 1995) Policies can of course fail to succeed and this happen when; (i) they are viewed as mere symbolic gestures, (ii) when teachers actively resist policy based change that see as imposed from the outside without their input or participation, (iii) when they do not have explicit connections to instructional practice (e.g. focus on hardware rather than their relationship to pedagogy), and (iv) then there is lack of programme and resource alignment to the policies intensions (Cohen & Hill, 2001; Tyack & Cuban, 1995).

According to (Phaopeng, 2010) posts that the term policy implementation has been defined by many scholars in association with the meaning of public policy implementation can be viewed only from a particular perspective but also from various dimensions as a number of remarkable scholars. Phaopeng (Phaopeng, 2010) in his findings observed that users name and passwords being changed periodically (at most monthly) and only authorized person having access to specific details of given information. Access Control Mechanisms respondents were asked to provide feedback on the extent to which the respective Colleges of Education they work for access control mechanism. As to whether all college staff had access to computers. Majority of respondents strongly agreed that (92.11%).While minority agreed (7.02) and strongly disagree (0.88%). As to whether Usernames and passwords were changed periodically majority of college ICT Staff agreed (61.54% followed by those who strongly agreed (26.32%) and only a few reporting not to be sure(4.39%) and disagreeing(1.75%) As regards all non-system administrator staff having limited access to ICT information from any computer. Majority of respondents strongly agreed (55.26%) followed by those who agreed (39.47% and lastly those who were not sure (5. 26%). By implication this means majority of the Colleges of Education staff are computer literate base on ICT. But as regards non-system administration there is need to engage them in capacity building. Training and awareness on ICT Implementation so as to move the organization forward.

Terms and Conditions of ICT Usage

(Siddiquah & Salim, 2017; UNESCO, 2014, 2015) points out that all staff are required to agree to the terms and conditions of staff acceptable use of ICT facilities agreement when receiving a computer account signifying, they have read and agree to abide by conditions outline in "Agreement". The findings of this study is consistent with that of (UNESCO, 2014, 2015) pertaining to having a provision for all staff to sign agreement on terms and condition of using ICT facilities only half of the condition of using ICT facilities only half of the respondents strongly agreed (50%). While the rest agreeing (46.69%) and the least ere not sure (3.51%)

As regards only employed staff having access to ICT facilities the highest proportion strongly agree (48.25%) and (43.86%) with 7.89% reporting not sure. The study is consistent with (Khan, 2012; Peltier, 2012) who found that terms and conditions of ICT usage affects the level of staff responsibility towards ICT infrastructure. This is because staff are expected to take full responsibility for activities conducted using computer and network accounts therefore must not allow anyone to use any of these accounts. This implies that all facilities provided by institution to staff members remain the property of the institution at all times. However, it remains the responsibility of staff to take care of them and be accountable to their use. As to whether all terminated staff must return all ICT facilities in their possession to the college management majority agreed (64.91%) followed by those who agree (28.95%) nand lastly those who were not sure (6.14%).

This study is consistent with the view of university of Portsmouth (Portsmouth, 2018) on termination of relationship; it is staff member responsibility to remove all personal data and e-mail including any personal intellectual property (as defined by the intellectual property policy) from their accounts. Staff should make arrangement for all institution data to be made available to other employees. If there is data or email remaining in a staff account at time of termination, the institution may access and use such data for legitimate purposes. Regarding the college reserving the right without notice to limit or restrict any individual's use and to inspect, copy, remove or otherwise alter data files or system resource which is used in violation of college rules or policies. The literature is in agreement with (UNESCO, 2014, 2015) points out that all staff are required to agree to terms and conditions of use of ICT facilities.

Data Backup Mechanism

The ICT Data Backup and Recovery Mechanism policy is created to guide and assist an institution to align with internationally recognize best practices regarding data backup recovery controls and procedures. This study reviewed this critical component of information security in the following aspects.

A scheduling back to run after working hours: In this respect, the majority of the respondents agreed at (51.75%) followed by those who strongly agreed (45.6%) and lastly those who were not sure (2.63%). This conforms to the best practise.

Existence of persistent Backup frequency (daily, weekly, monthly) in the colleges of education; the study investigated if there exist a persistent culture for backing up data at a given interval. The study revealed that the majority of the respondents strongly agree (63.16%) with the rest agreeing (34.21% or reporting that they were not sure (2.63%)

Documentation of backup procedures and updated regular. In this line of investigation, the highest proportion of respondents strongly agreed at (52.63%) and agreed (43.86%) with (3.51% reporting not sure. This practise strongly agreed with the best practise that stress and emphasis the purpose of auditing and control of backup data.

Assignment of duty for data backup to system administrator; in this respect highest proportion of respondents strongly agreed at (57.02%) followed by those who agree (39.47%) and lastly those

who were not sure (3.51%). This study's findings agree with Parrish (2013) who emphasized the role of system administrator in colleges while advocating that professionalism should never be compromised for quality. Therefore, system administrator must be allowed to use his expertise in promoting a good back up system.

Pertaining to whether external expertise is sought in order to recover critical data the highest proportion of respondents strongly agreed (40.35%) and agreed follow by those who were not sure (16.67%) of those disagree (1.75%) and lastly those who strongly disagree (0. 88%). In this respect we note that the field of information management systems is very complex and the systems administrator might not be having all the required expertise. Therefore, there is need to sought professionals in order to recover critical data when the system is faulty. However, the system administrator must work hard with other professional colleagues to rectify the problem.

Disaster Recovery Plan (DRP) Mechanism

The study investigated the DRP in colleges of education in three directions as follows.

Turnaround time to receive a backup for recovery; the study found out that 2 hours was the maximum turnaround time in most of the colleges of education. Accordingly, the highest proportion strongly agree at (51.75%) and agree (4.86%) and not sure at (4.39%).

Regular testing of backup media; according to the international best practises, backup media should be regularly tested to ensure that they can be relied upon for emergency use. The highest proportion of respondents strongly agreed (54.39%) and agreed (42.11%) with only (3.51%) not sure.

Restoration time frame; best practises recommend that restoration procedures should be regularly checked and tested to ensure that they are effective and can be completed within recovery time allotted in operational procedures for recovery. In respect of the respondents feedback, the highest proportion of the respondents strongly agreed (55.26%) and agreed (42.11%) with only (2.63%) not sure

The study found that the respondents assessed recovery plans is very satisfactory. This was demonstrated by the fact that ICT departments ensured regular back up of every running server appropriate level of physical and environmental protection restoration procedures checked and tested to ensure that they are effective. Calder and Watkins (Calder & Watkins, 2010; Calder & Watkins, 2015) agree that the main aim of ICT Disaster Recovery Plan(DRP) is to ensure that should the organization / Institution experience disaster of any nature (e.g. Fire outbreak, power surge or building is damaged etc.) the organization/ institution has emergency contingency plans for backup systems). In other words, such plan is to make staff aware of what procedures should be followed when connecting backup systems and who the key contact persons for the systems are. The Disaster Recovery Plan (DRP) is therefore there to ensure a Disaster Recovery Team of the College is appointed and trained properly so that even if IT staff is not in the office the team can take charge successfully.

This therefore implies that once a disaster is declared by the College Management and a decision is made to invoke the Disaster Recovery Plan, the ICT Disaster Recovery Team can obtain backups from offsite secure storage, install security systems that are applicable and packages set up computers provide other users support and assist where possible with email and internet services.

CONCLUSION

The study established that ICT policies have been implemented to a great extent in most of the surveyed colleges of education. Similarly, the most basic security mechanisms have been implemented for example the use of password and usernames. In the same light the implementation of ICT policies was found to significantly affect the level of information security. This is because establishing access control mechanisms ensure data confidentiality, integrity, availability, non – reputation and auditability of information. Defining terms and conditions of using college ICT facilities and services from different categories of users help to ensure data confidentiality and availability and shows good association between ICT policy implementation and information security in terms of performances and developing and implementing appropriate backup and recovery mechanisms for institutional data helps to ensure data availability and developing and implementing ICT disaster recovery plan helps to ensure data availability.

All in all, therefore it can be concluded that good implementation of ICT policies is a pre- requisite for high level performance of information security, However, if policies are not well implemented to cater for information security aspects of the colleges then the likelihood of ensuring that the five pillars of information security will be low.

RECOMMENDATIONS

The following recommendations are way forward to achieve viable ICT policy implementation and information security.

ICT personnel need to be trained on regular bases to sharpen and enhance their knowledge on new threats to information security. This can be done through ICT workshop retreats, seminar and symposium.

The staff and students must be regularly supported guided and trained by ICT personnel on how to ensure information security of ICT facilities. They can be taught about topics such as antivirus installation, passwords, portable media devices, back up, social media internet usages, internet scams and email scams.

The Federal Government of Nigeria must promulgate legislation on cybercrime Act and offenders must be punished.

Terms and condition of ICT usage must be strictly followed. All staff using ICT facilities must mandatorily sign an “Agreement form “for them to have access to the ICT system.

The Federal Government of Nigeria must embrace the new technology of Public key Infrastructure (PKI) of encryption of information in ICT systems.

REFERENCES

Adebowale, O. F., & Dare, N. O. Teachers' Awareness of Nigeria's Educational Policy on ICT and the use of ICT in Oyo State Secondary Schools. *International Journal of Computing and ICT Research, 6*(1), 84-93.

ATSB, A. T. S. B. (2013). Reliability of Robinson R22 helicopter belt drive system ATSB. *ATSB Transport Safety Report, Aviation Occurrence Investigation, AI-2009-038*.

Avolio, F. M., & Fallin, S. (2007). Producing Your Network Security Policy. *Watchguard Technologies, Inc.*, 1-13.

Bayuk, J. (2009). How to Write an Information Security Policy. *Computerworld*. Bell, D. E. (2006). *Looking back at the Bell-La Padula model* (Vol. 2005).

Bryman, A. (2006). Integrating Quantitative and Qualitative: how is it done? . *SAGE Publications, 6*(1), 97-113. doi:https://doi.org/10.1177/1468794106058877

Burns, R. B. (2018). Validity and reliability assessment of qualitative research.

Calder, A., & Watkins, S. G. (2010). ISO27000 and Information Security: A Combined Glossary.

Calder, A., & Watkins, S. G. (2015). IT Governance: A Manager's Guide to Data Security and ISO27001/ISO27002.. *London: Kogan Page Limited*.

Cohen, D. K., & Hill, H. C. (2001). Learning Policy: When State Education Reform Works. *New Haven: Yale University Press.*

Creswell, J. W. (2011). Educational Research: Planning, Conducting and Evaluating Quantitative and Qualitative Research. . *4th Edn., Pearson Education, Boston, ISBN-10: 0132613948,*, pp: 650.

Creswell, J. W. (2012). Educational research: Planning, conducting, and evaluating quantitative and qualitative research. *Upper Saddle River, NJ: Prentice Hall*.

Diver, S. (2007). Information Security Policy – A Development Guide for Large and Small Companies. *SANS Institute. South Africa.*, 1-43.

Flowerday, S., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & Security, 61*, 169-183. doi:10.1016/j.cose.2016.06.00

Freebody, P. (2003). Qualitative research in education: Interaction and practice *London: Sage.*

Garba, S. A., Singh, T. K. R., Yusuf, N. B. M., & Ziden, A. A. (2013). An Overview of ICT Integration in Nigerian Colleges of Education and the Implications on Social Studies Pre-Service Teacher Training Programme: A Review of the Literature. *Journal of Education and Learning, 7*(1), 35-42.

Hee, O. C. (2014). Validity and Reliability of the Customer-Oriented Behaviour Scale in the Health Tourism Hospitals in Malaysia. *International Journal of Caring Sciences, 7*(3), 771-775.

Hong, K.-S., Chi, Y.-P., Chao, L., & Tang, J.-H. (2006). An empirical study of information security policy on information security elevation in Taiwan. *Information Management & Computer Security, 14*. doi:10.1108/09685220610655861

Hong, K.-S., Chi, Y.-P., Chao, L. R., & Tang, J.-H. (2003). An integrated system theory of information security management. *Information Management & Computer Security, 11*(5), 243-248. doi:https://doi.org/10.1108/09685220310500153

Jackson, S. L. (2009). Research Methods and Statistics: A Critical Thinking Approach 3rd edition. *Belmont, CA: Wadsworth.*

Johnson, R. B., & Christensen, L. (2014). Educational research: Quantitative, qualitative, and mixed approaches, Fifth edition. *SAGE Publications*, 621.

Jones, R. (2003). Local and national ICT policies. In: R. Kozma (ed.), Technology, Innovation, and Educational Change: A Global Perspective., 163-194.

Kearney, W., & Kruger, H. (2013). Effective corporate governance: Combining an ICT security incident and organisational learning. *The 2nd International Conference on Cyber Security, Cyber Peacefare and Digital Forensic (CyberSec 2013)*, 12-21.

Khan, K. (2012). Present status of information communication technology (ICT) and infrastructure facilities in high court libraries of India. *International Journal of Library and Information Science, 3*(5), 81-87. doi:10.5897/IJLIS11.081

Kozma, R. (2005). National policies that connect ICT-based education reform to economic and social development. . *Human Technology, 5*(4), 358-367.

Kruger, H., & Kearney, W. (2008). Consensus ranking - An ICT security awareness case study. *Computers & Security, 27*, 254-259. doi:10.1016/j.cose.2008.07.001

Lazo, J. (2010). An Overview of Qualitative and Quantitative Method. *National Center for Atmospheric Research. INCOMPLETE*.

McClelland, R. (2010). The Protective Security Policy Framework (PSPF), https://www.protectivesecurity.gov.au/. *Australian Government*.

Morse, J. (2003). Principles of mixed methods and multi method research design. *London; Oxford University Press*.

Mugenda, O. M., & Mugenda, A. G. (2003). Research Methods: Qualitative and Quantitative Approaches. *Nairobi: Africa Center for Technology Studies.*

Okesola, J. O., Onashoga, A., & Ogunbanwo, A. (2016). An investigation into users' information security awareness on social networks in south western Nigeria. *SA Journal of Information Management, 18*(1). doi: https://doi.org/10.4102/sajim.v18i1.721

Onen, D. (2016). Appropriate Conceptualisation: The Foundation of Any Solid Quantitative Research. *The Electronic Journal of Business Research Methods, 14*(1), 28-38.

Peansupap, V., & Walker, D. H. T. (2006). Information communication technology (ICT) implementation constraints. *Engineering, Construction and Architectural Management, 13*(4), 364-379. doi:https://doi.org/10.1108/09699980610680171

Peltier, T. R. (2012). Information Security Policies, Procedures, and Standards: guidelines for effective information security management. *Boca Raton, FL: Auerbach publications.*

Phaopeng, P. (2010). The Success of ICT Policy Implementation in Education: Evidence from Upper Level Secondary Schools in Thailand. Doctoral dissertation, National Institute of Development Administration.

Portsmouth, U. o. (2018). All University of Portsmouth staff receive a computer account that enable access to university computer facilities. How to get your staff computer account.

Saunders, M., Lewis, P., & Thornhill, A. (2007). Research Methods for Business Students, 4th Edition *Harlow: FT Prentice Hall.*

Schlienger, T., & Teufel, S. (2002). Information Security Culture: The Socio-Cultural Dimension in Information Security Management. *Conference: Proceedings of the IFIP TC11 17th International Conference on Information Security: Visions and Perspectives*.

Sekaran, U. (2003). Research Methods for Business, a skill building Approach. . *USA: Hernitage Publishing Service.*

Sekaran, U., & Bougie, R. (2016). Research methods for business: A skill building approach (7th ed.). *Chichester, John Wiley & Sons.*

Siddiquah, A., & Salim, Z. (2017). The ICT Facilities, Skills, Usage, and the Problems Faced by the Students of Higher Education. *Eurasia Journal of Mathematics, Science and Technology Education, 13*(8), 4987-4994.

Stevens, J. P. (2009). Applied Multivariate Statistics for the Social Sciences *Taylor & Francis*.

Tella, A. (2011). Availability and Use of ICT in South-Western Nigeria Colleges of Education. *African Research Review: International Multidisciplinary Journal, 5*(5), 315-331.

Trochim, W. M. (2007). The Research Methods Knowledge Base

Tuyikeze, T., & Flowerday, S. (2014). Information Security Policy Development and Implementation: A content analysis approach. *Conference: 8th International Symposium on Human Aspects of Information Security and Assurance(HAISA)At: Plymouth, United Kingdom Conference International Symposium on Human Aspects of Information Security & Assurance*.

Tyack, D., & Cuban, L. (1995). Tinkering toward Utopia: A Century of Public School Reform. *Cambridge, MA: Harvard University Press.*

UNESCO. (2014). Information and communication technology (ICT) in education in Asia: A comparative analysis of ICT integration and e-readiness in schools across Asia. . *Montreal: UNESCO Institute for Statistics., Information paper no. 22*.

UNESCO. (2015). Information and communication technology (ICT) in education in Sub- Saharan Africa: a comparative analysis of basic e-readiness in schools. *UNESCO Institute for Statistics, UIS/2015/ICT/TD/5* (REV.2), 1-30.

Yushau, B., & Nannim, F. A. (2018). ICT Facilities and their Utilization for Educational Purpose in Nigerian Universities: A Review of Literature from 2004 to 2018. *ATBU, Journal of Science, Technology & Education, 6*(1).

Yusuf, M. O. (2005). Information and communication technology and education: Analysing the Nigerian national policy for information technology. *International Education Journal, 6*(3), 316-321.

Yusuf, M. O. (2007). Trends and barriers on the integration of information and communication technology in the Nigerian school system. *A Publication of Curriculum Studies and Instructional Technology*.