THE STATE OF INFORMATION SECURITY IN SOUTH-WESTERN NIGERIAN EDUCATIONAL INSTITUTIONS

Sodiya A. S*. Ibrahim S. A. and Ajayi O. B.
Department of Mathematical Sciences, University of Agriculture, Abeokuta.
(*Corresponding author; Email: sinaronke@yahoo.co.uk)

ABSTRACT

Information security is now a critical issue in academic and business communities today. This paper addresses the issue of information security and the state of information security as it affects academic research activities in eight government universities in South Western Nigeria. A sample of 336 respondents (response rate = 100%) was taken among all levels of academic staff in the targeted institutions. The results from the analysis of data gathered through the use of questionnaire showed a poor state of information security in institutions. The work was concluded while stating what to be done to improve the situation and meet the future challenges in information security.

Keywords: Information, Information security, Educational institutions, Future challenges

INTRODUCTION

Information security has been an active research area for more than two decades, but has recently become a matter of serious concern even among ordinary users of computer system. This is because more and more individuals or organizations now rely on computer systems for their day-to-day information storage and processing. Also, computers are now trusted to keep and manage sensitive information. With this increasing dependence on computing systems in today's society; the security of the systems has become an essential issue and has finally started to attract public interest.

From the foregoing, information technology is a fruitless effort if there is no security. If information that has been gathered over a period of time can just be accessed, stolen or modified in just one second, which renders all efforts useless. Information security concerns the protection of information technology (IT) systems against attacks. An attack is an intentional threat and is an action performed by an entity with the intention to violate security policies. Examples of attacks are destruction, modification, fabrication, interruption or interception of data (Pfleeger, 1989)

However, in Nigeria educational institutions, computer system are subject to wide range of mishaps – ranging from corrupted data files, viruses, to natural disasters and unauthorized access to personal academic data and vital institutions' information. The overall objective of this work is therefore, to examine the present state of information security in Nigeria institutions so as to improve the security of existing and future systems. The specific objectives of the study are:

i) To determine whether security breaches are experienced on academic research data or information
ii) To identify the common causes of security breaches in institutions
iii) To identify the security breaches preventive mechanism commonly used
iv) To determine the frequency of update or maintenance of the preventive mechanism
v) To assess the existence of information security policies in educational institutions
vi) To identify the sources of information security information of security breaches

Information security technology issues

The basic issue in IT security is making IT resources and services available only to those who are authorized to have them. It also encompasses the authority to manipulate the resource or service function as appropriate. For example, the user of an IT resource (say a file) may have authority to access the resource (i.e. read the file) but may not have authority to modify (i.e. write into, delete the file, etc) and / or transmit the resource over the network (i.e. send the file to another local or remote system). A good IT security system should not only disallow unauthorized users from accessing resources, it must also never disallow an authorized user from accessing the system resource if and when such resource of service is available. Thus, IT security system must:

Deny unauthorized user access to resources and services available on the IT system.
Allow authorized users to carry out only functions that have been allocated to them by the IT system inistrator.
Must never deny an authorized user the use of a resource or service, which is available on the IT system.
Summarily, computer security is primarily concerned with protecting computer resources from unauthorized s (Olovsson, 1992). The value of these resources can be compromised in three ways commonly referred the CIA's of computer security;

Confidentiality: - Prevention of unauthorized disclosure of information
Integrity: - Prevention of unauthorized modification of Information
Availability: - Prevention of unauthorized withholding of information

In order to maintain these policies, many mechanisms have been put in place but the problem still persists. of these mechanisms are the use on antivirus, authentication and identification, audit trail, firewalls and sion detection systems. Most of these intrusion prevention mechanisms are good but the state of information rity in our environments is alarming. The situation is even worse when the resources/service available on system has high values. In educational institutions, student records, institution information and academic arch data or information are some of the IT resources that carry high risk of being illegally accessed. refore, it is important to use all the possible and available technology to secure IT system and the resources/ vices held in them.

lated works

The field of information security has not yet begun to mature in Nigeria, and it might not even mature, as e would like to see. After all, the information security teams are always playing catch-up to other major chnologies. Until the discipline is developed and priority is given to protection of all our information systems, curity will always fall short of the dream.

Most highly placed educational institutions in Nigeria still experience computer break-in even with the ct that they have a computer science (IT) department. Generally, 82 percent of organization in Nigeria still perience computer intrusion (Sodiya *et al*, 2003). Ernst and Young, (2002) found out that 75 per cent of ganizations experienced some forms of interruption on valuable information. 90 per cent of organizations rge corporations and government establishments) reported computer security breach in the last 12 months.

Sigmond and Kaura (2001) reported that the rising frequency of security incidents is increasing spending IT security. Concerns over security and associated issues continue to be listed as a top challenge. Angell, 96) reported that there are extensive evidence to suggest that the threats to security of information are owing in number and variety and most importantly, the severity of their impact. (BSI, 1999) emphasized the portance of information security policy and considered it as a document of strategic importance in organization. any surveys on information security are now taking information security policies as important (Anderson, 001, Ernst & Young, 2001, DTI, 2002). Haggins, (1999) stated that without security policies, security practices ould be developed without clear demarcation of objectives and responsibilities.

ETHODOLOGY OF DESIGN

mple Characteristics

e population for this study consists of academic staff of all government universities in outh-West Nigeria. A random sample that cut across all levels of academic staff (7 levels) as made.

Table 1: Showing the arrangement of sample taken per institution

AcademicLevels	Disciplines Science	Social Science	Engineering	Art	Agriculture	Medicine &Pharmacy	Total
GraduateAssistant	1	1	1	1	1	1	6
Assistant Lecturer	1	1	1	1	1	1	6
Lecturer II	1	1	1	1	1	1	6
Lecturer I	1	1	1	1	1	1	6
SeniorLecturer	1	1	1	1	1	1	6
Reader	1	1	1	1	1	1	6
Professor	1	1	1	1	1	1	6
Total	7	7	7	7	7	7	42

The total number of sampled universities is eight. Therefore, the total sample size for this study is 336

Data collection

Data was collected through the use of questionnaire. The detailed questionnaire, which sought to explore the stated research objectives, was designed, validated, and ultimately executed.

Questionnaire Development, validation and targeting:

A draft questionnaire was developed and organised into the following sections:

i. *Personal Information*: The information includes the name of the institutions, the discipline, years of experience and position of the academic researcher. This information was collected so that the potential moderating effec on the statistical analysis could be explored.

ii *Information Security Information*: This section was designed in order to evaluate the scope of informatio security institutions. Also, to check the factors that is affecting the success of the information security. It als sought to determine whether institutions have a documented security policy and if it did, what kind of securit breaches protective mechanisation do they experience.

The draft questionnaire was initially validated through a series of pre-tests, first with 6 professors from al the disciplines. The suggestions at this pre-test stage led to some modifications of the instrument. The instrumen was then re-tested again with 7 (one from each level) academic researchers in all the disciplines. The pre-tests were very useful, as they resulted in a number of enhancements being made to the structure of the survey and the construction of specific questions. Having refined the questionnaire, the full survey was then under-taken, which provides the needed data for analysis. Total questionnaire administered was 336 and the response rate was 100%.

Methods of data analysis

The objectives were analysed using frequency counts and the hypotheses tested using chi-square method.

RESULTS AND DISCUSSION

Table 2: Coverage of Information Security Technology in Institutions.

Coverage of Information Security Technology	Yes	No
a. Use of personal computer for academic research	225 (67%)	111 (33%)
b. Experiencing of security breaches on academic research data or information	290 (86%)	46(14%)
c. Connection of Computer system to network	136 (40%)	200 (60%)
d. Existence of information security policy in institutions	61 (18%)	275 (82%)
e. Existence of information security awareness programme in institutions	57 (17%)	279 (83%)

* The figures in the parenthesis represent percentages

Table 3: Common sources of security breaches experienced		
Common sources of security breaches in institutions	Freq.	%
Virus and Worms	147	44
Unauthorised access to files and system resources	122	36
Errors in system or network configuration	67	20
None	0	0

Table 4: Frequently used security breaches preventive mechanism		
Most frequently used security breaches preventive mechanism	Freq.	%
Anti-virus	237	71
Authentication and identification	51	15
Firewalls	18	5
Intrusion Detection System	1	0..3
None	29	8.7

Table 5: Level of update or maintenance of the preventive mechanisms		
Frequency of update or maintenance to the preventive mechanisms	Freq.	%
High	4	1
Average	50	15
Low	231	69
None	51	15

Table 6: Common sources of security information		
Sources of security information	Freq.	%
Office	68	20
News, newspapers, posters, bulletins	64	19
Books & Journals	19	6
Internet	65	19
None	120	36

Hypotheses Testing

Hypothesis I:

Table 7: Contingency table showing relationship between discipline and nature of security breaches experienced

Discipline	Security Breaches			
Discipline	Virus And Worms	Unauthorised Access	Errors In System Or Network Configuration	TOTAL
Science	23 (24.5)	22 (20.3)	11 (11.2)	56
Social Science	22 (24.5)	29 (20.3)	5 (11.2)	56
Art	18 (24.5)	15 (20.3)	23 (11.2)	56
Agriculture	23 (24.5)	20 (20.3)	13 (11.2)	56
Medicine And Pharmacy	37 (24.5)	17 (20.3)	2 (11.2)	56
Engineering	24 (24.5)	19 (20.3)	13 (11.2)	56
TOTAL	147	122	67	336

With df = 10, $\div^2_{0.05}$ = 18.31 and $\div^2_{cal}$ = 38.427,

Decision: Since $\div^2_{cal} > \div^2_{0.05}$, H_0 is rejected

Summary of Findings

a). 67% of respondents use personal computers for academic research, which shows that many institutions are yet to provide computers for academic staff

b). 86% of the respondents experience security breaches on academic data or information, which signifies a major security problem for academia

c).40% have their computers connected to network. Computers that are connected to networks are believed to face more security problems.

d). 82% have no IT security policy in place in their institutions. This might be one of the reasons why security breaches are so on the high side in the institutions

e). 83% have no security awareness programme. Security awareness programme is supposed to be part of security policy. If security policy is not in place, we should at least create awareness within the institutions

f). The common sources of security breaches are stated in table 3 with virus and worms having the highest percentage (44%).

Hypothesis II:

Table 8: Contingency table showing relationship between job position and frequency of security breaches experienced

Job Position	*Frequency of Security Breaches Experienced*				TOTAL
	More Frequently	Frequently Frequently	Less	Rarely	
Professor	20 (0.047)	24 (1.704)	3 (2.285)	1	48
Reader	21 (0)	18 (0.008)	9 (0.571)	0	48
Senior Lecturer	25(0.761)	20 (0.139)	3 (2.285)	0	48
Lecturer 1	31 (0.4761)	15 (0.628)	1 (5.124)	1	48
Lecturer 2	14 (0.2333)	16 (0.313)	14 (7.00)	4	48
Assistant Lecturer	18 (0.428)	19 (0.019)	9 (0.571)	2	48
Graduate Assistant	18 (0.761)	17 (0.106)	10 (1.285)	3	48
TOTAL	147	129	49	11	336

With df = 18, $\div^2_{0.05}$ = 28.87 and $\div^2_{cal}$ = 39.819,

Decision: Since $\div^2_{cal} > \div^2_{0.05}$, H_0 is rejected

Hypothesis III:

Table 9: Contingency table showing relationship between level of computer literacy and frequency of security breaches

Level Of Computer Literacy	*Frequency of Security Breaches*				
	More Frequently	Frequently	Less Frequently	Rarely	Total
High	62 (64.75)	64 (56.82)	19 (21.58)	3 (4.84)	148
Average	46 (52.06)	53 (45.68)	15 (17.35)	5 (3.89)	129
Low	38 (27.56)	10 (24.18)	14 (9.187)	1 (2.06)	63
None	1 (2.625)	2 (2.30)	1 (0.875)	2 (0.19)	6
Total	147	129	49	11	336

With df = 9, $\div^2_{0.05}$ = 16.92 and $\div^2_{cal}$ = 38.177,

Decision: Since $\div^2_{cal} > \div^2_{0.05}$, H_0 is rejected

g). The common preventive mechanisms used are stated in table 4, with the Anti-virus (71%) being the commonest.

h) The level of maintenance to these preventive mechanisms is generally low (From Table 5)

i) The largest percentage (36%) have no access to security information (From Table 6)

j)There is no significant relationship between discipline and nature of security breaches experienced (From Table 7)

k)There is no significant relationship between job position and frequency of security breaches (From Table 8)

l) There is no significant relationship between level of computer literacy and frequency of security breaches (From Table 9)

The requirements for meeting the future challenges in information security

The underlying information security technology needs to be improved so that a friendly environment can be created for research and teaching in the country. However, in achieving this, the followings have to be considered in achieving secured computing environment.

i. *Policies and Laws*: There is need to have established policies on information security in the institutions. In the general terms, there is a need to make significant improvement in our legal infrastructure to foster better information security. This includes laws and policies that allow law enforcement to respond to information attacks in real time across the world. It could also mean some form of regulation to standardize and impose some minimum level of mandatory detection, reporting, and investigation of events.

ii. *Awareness*: Awareness simulates and motivates users to care about security and to remind them of important security practices. For example, explaining what the consequences would be if information security information is ignored might motivate people to take security seriously. There should be a continuous security awareness programme so that people would always be informed about new security techniques and solutions.

iii. Training: The purpose of training is to teach people the skills that will enable them to perform their jobs more securely. This includes teaching people what they should do and how they should (or can) do it. Advanced training must be provided to people that are charged with IT responsibility. Also, there periodic training must be targeted for all staff in institutions to advance their skills in information security. In teaching general users, care should be taken not to overburden them with unneeded details. The training should be made useful by addressing security issues that directly, affect the users. The goal is to improve basic security practices, not to make everyone literates in all the jargon or philosophy of security.

iv. Education: Security education is more in-depth than security training and is targeted for security professionals and those whose jobs expertise is security. Security education is normally outside the scope of most organization awareness and training program.

As part of the security education, the Nigerian University Commission should include Information security as a core course in the curriculum for those in the field of computer science. This area must be directly focused on because it has been one of the reasons why most organizations do not take security seriously.

v. *Be in-touch with current techniques*: Information security is a vast and dynamic discipline of computer science. There are new hackers and intruders techniques everyday and hence, the need to abreast ourselves in this country to development. Also, there are always new security designs every time to move towards efficiency. So, everybody in academic institutions and other organizations that are responsible for maintaining sensitive information should always be in-touch with current techniques.

vi. *Information security should be periodically re-accessed* : Computers and the environments they operate in are dynamic. System technology, users, data and information in the system, risks associated with the system, emergency of a new threat and security requirements are very-changing. This calls for the need to always access the state of the art of information security so as to plan effectively with these changes.

In addition, security is never perfect when a system is implemented. System users and operators discover new ways to intentionally or unintentionally bypass or subvert security. Changes in the system or the environment can create new vulnerabilities. Strict adherence to procedures is rare, and procedures become outdated over time. All of these issues make it necessary to re-access the security of information periodically.

CONCLUSION

While information technologies are stable and quite powerful, there are of course still needs and desires among the users' community in terms of security. Our findings show a poor state of information security in the sampled institutions. We need to develop the discipline and priority needed to instil strong security underpinnings in all our information systems so that security will not fall short of the dream.

Additionally, security problems can affect morale of staff, which would consequently, affect research and teaching activities. Management of institutions should be fully involved in providing information security. If the support of management were not adequate, it would be difficult to attain the desired height in information security.

Our findings show a poor state of information security in the sampled institutions, which will consequently affect productive research in higher institutions. Productive research promotes national growth or development. It is then a critical situation if academic research documents, files, data and results are not secured. Therefore, attention to the suggested solutions would greatly be appreciated. There is need to improve information security in Nigeria institutions. All efforts should be geared towards achieving this. We also advise that government should give all bodies of IT in this country adequate support so that the future of information security technology would be generally guaranteed in Nigeria.

REFERENCES

Angell, I. O. (1996), "Economic crime: beyond good and evil", *International Journal of Financial Regulation & Compliance,* Vol. 4 No 1, UK.

British Standards Institute (BSI) (1999), Information Security Management – BS 7799-1:1999, BSI, London.

Caelli, William, Dennis Longley, and Michael Shain (1991). *Information Security Handbook* . New York, NY: Stockton Press

Charles P. Pfleeger (1989). "Security in Computing", *Prentice Hall International,* Inc. ISBN 0-13799016-2.

Department of Trade and Industry (DTI) (2002), "Information Security Breaches Survey 2002", *Technical Report*, April, DTI, London

Ernst & Young (2001), "Information Security Survey", Ernst & Young, London.

Ernst & Young (2002), "Global Information Security Survey", Ernst & Young, London.

Haggins, H. N. (1999), "Corporate System Security: towards an integrated management approach", *Information management and computer security,* Vol. 21, No 5, Uk.

NIST Handbook Special Publication (2002). "An Introduction to Computer Security", Pul: 800-12

Olovsson Tomas (1992). "A Structured Approach to Computer Security", *A Technical Report No 122*, Department of Computer Engineering, Chalmers University of Technology, Gothenburg, Sweden.

Odejobi, O. A. & Ayeni, J. O. A. (2002) "Trends in Speech Technology and its implication for IT system security", *COAN conference a series,* volume 13, pages 167-176.

www.securityfocus.com: Technical and newsworthy security information.

Russel, Deborah, and G.T. Gangemi (1991) "Computers Security Basics", Sebastopol, CA: O'Reilly & Associates, Inc., 1991.

Sigmond, S. and Kaura, V. (Ed.) (2001), "Safe and sound – a treatise on Internet security", *RBC Capital Markets*, November

Sodiya A.S., Ajayi O. B., Okunlaya S. A. (2003). "Intrusion detection system: A panacea to computer security problems", Accepted for publication in *Journal of production and research,* Enugu.

U.S. Department of Energy Computer Security Awareness and Training (1998). Guideline (Vol. 1). Washington, DC. DOE/MA-0320 Feb. 1988.