Cyber-Security of Higher Institution Web Portals in Nigeria

Article · September 2021

CITATIONS
0

READS
9

1 author:

Victoria Adebimpe Akano
Crawford University
5 PUBLICATIONS **34** CITATIONS

SEE PROFILE

Crawford Journal of Natural & Applied Sciences 1
(2019) pp 245-251

CJNAS Vol 1
A Publication of Crawford University College
of Natural and Applied Sciences

Crawford
Journal of Natural &
Applied Sciences

Cyber-Security of Higher Institution Web Portals in Nigeria

Victoria A. Adewale
Department of Computer and Mathematical Sciences, Crawford University
Faith-City, Igbesa, Ogun State, Nigeria
bimpsyade@gmail.com
victoria.adewale@crawforduniversity.edu.ng
Tel: +2347066240208

Received 24th April, 2019; Accepted 29th August, 2019

Abstract

Every institutional web portal should be treated as a *"jewel in a crown"*. The reason for this cannot be far-fetched in that, each institution has two basic assets to guard jealously, which is the identity of the university and its clienteles. The drive for this research on institutional portals can be attributed to the fact that the portal serves as the first point of entry in most cases to the clienteles in order to provide essential information and application resources in a secured, consistent and reliable mode. However, this treasure chest of high value information is vulnerable in most cases to cyber-attacks resulting from unintended disclosure of vitals through phishing, improper use of social media and supposed availability of services. There is therefore the need to do a better job not only of bolstering network defenses against cyber-attacks, but also of raising awareness of basic cyber security hygiene among the full spectrum of IT users: the university and its clienteles. This study gives different approaches on tools, tactics and procedures of minimizing the number of compromised networks and stolen data.

Keywords: Portal, Cyber-security, Cyber-attacks, University

1. Introduction

Tertiary institutions today no longer depend on manual information system but have embraced technology for automated information systems. Basically, universities employ web portals at different levels to perform several processes ranging from student information system to result processing system which are been hosted in the cloud for ease of use and access. With this in mind, portal development tends to focus more on functionality rather than security (Punch, 2017). Universities web portals issues may not be explicitly categorized under security but summed up as simple information system errors that can be resolved in no time which on the contrary turns out to be false. A reliable but insecure web portal will only lead to an inefficient system or denial-of-service out rightly if not checkmated.

Higher institutional portals houses large variety of sensitive and lucrative data which makes them targets for past few years.(Carlos Soto, 2016)

Causes of Cyber-attacks in Tertiary Institutions

There are several factors that contribute to the cyber threats and attacks associated with institutional portals, but this study will focus on the germane ones as try to proffer possible solutions to them. These include:

1. Possession of high valued information
2. Extensive use of personal devices
3. Organisation susceptibilities
4. Decentralized structures

i. **Possession of high valued information:** Higher institutions of learning houses a wide variety of vital and sensitive information about staff, students, parents, alumni and that of entire system from the inception of the institution. This accumulated large volume of data makes it attractive to attackers to perform malicious activities.

ii. **Extensive use of personal devices:** As technology improves, the use of personal devices in organisation such as the institute of learning has increased greatly. Students, staff, visitors, colleges, and faculties make use of their smart phones, tablets, PCs for teaching, learning and other social functions. In the bid for these, several applications are installed; different sites are visited and malicious contents are downloaded on these personal devices which in most cases are not secured. These set of users invariably perform their regular organizational activities on same devices and unconsciously expose their institution to cyber risks by sharing sensitive data about the institution.

iii. **Organisation susceptibilities:** Every organisation has a structure by which it operates and the failure to implement the laid down structure will result in the dilapidation of the organisation. In this 21st century, higher institutions of learning use technology as the window to showcase their worth and values to the world and since technology is inevitable, there is the need to put up proper IT structure in institutions. The vulnerabilities of an institution arises when the management of the school has no IT official in its cabinet to ensure proper placement of the IT structure and prevent cyber insecurities of whatsoever technology the institution employs (EDUCASE, 2018). Also, institutions rarely see the need to train their clienteles on cyberspace and cyber-security as pertaining the pros and cons of usage.

iv. **Decentralised structures:** The vulnerabilities of organisation coupled with the decentralized structure of information storage in the university indirectly creates multiple paths for cyber-attackers to explore and retrieve whatever information they need from the institution since the information sought for can easily be accessed through the unsecured channels; faculties or colleges, departments, units or personal devices.

2. Methodology

This study employed the use of questionnaire for the survey to determine the causes, threats and possible solutions from cyber-attacks on university web portals. A total of twenty-two (22) higher institutions of learning (ten federal, nine state, and three private) participated in the survey. Students, alumni and staff of these institutions participated in the survey. Confidentiality of personal information was guaranteed as respondents were asked to give honest answers to items in the questionnaire.

3. Results and Discussion

The questionnaire was divided into two basic sections: demography and cybercrime, and from the survey, the

following intriguing results were obtained:

Section 1: Demography

Category and percentage of respondents

The number of respondents that participated in this survey totaled seventy-four. With staff, students, and alumni percentage as 24.24%, 71.21% and 4.55% respectively.

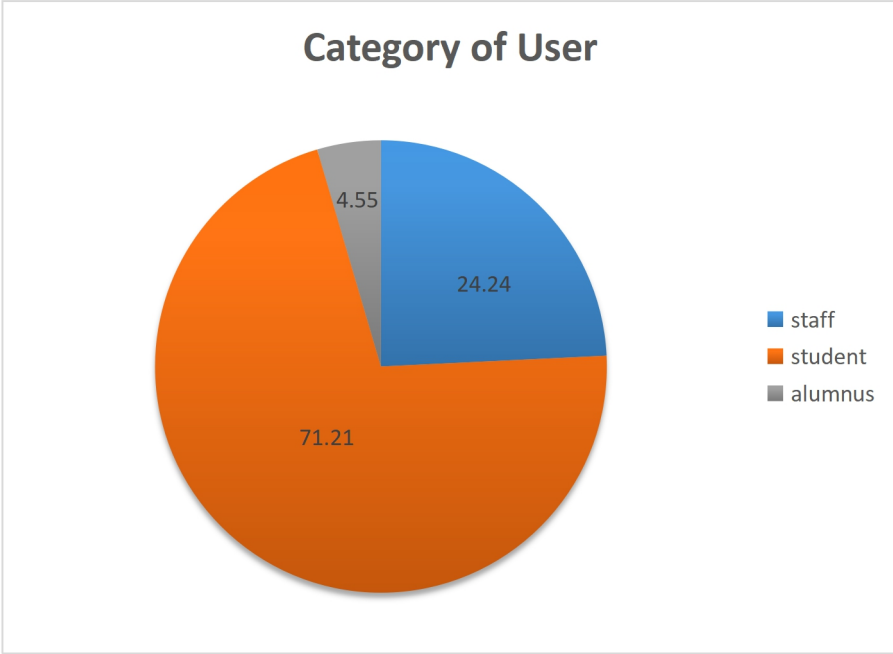

Figure 1: Category of respondents by occupation

The survey took a holistic view from the various types of higher institutions of learning: federal, state and private. The percentage of the participants by the type of institution is given as federal institutions 46%, state institutions 41% and private institutions 18%.

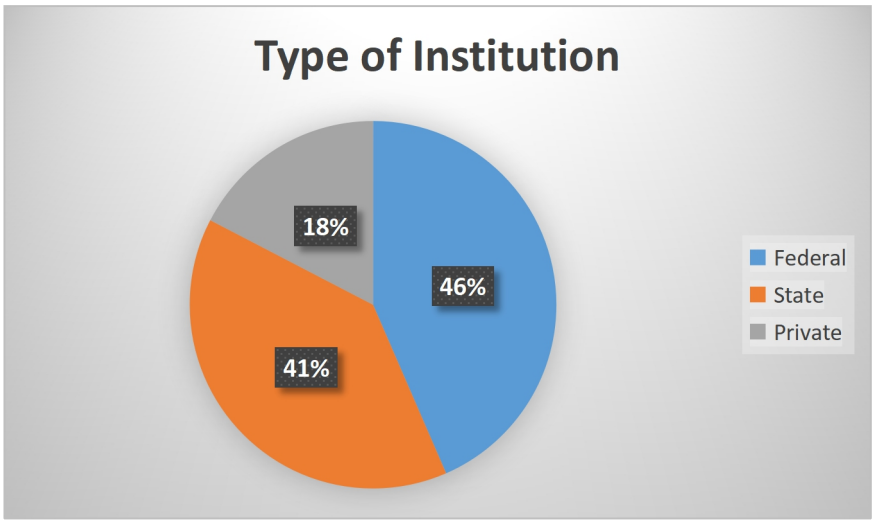

Figure 2: Category of respondent by Institution

Table 1: Participating Institutions

SN	Institution	Type
1	AAUA	State
2	Adeyemi College of Education	Federal
3	Babcock University	Private
4	Crawford University	Private
5	Ekiti State University	State
6	Federal College of Education, Abeokuta	Federal
7	Federal Polytechnic Ado- Ekiti	Federal
8	Federal School of Survey, Oyo	Federal
9	FUNAAB	Federal
10	FUTA	Federal
11	LASU	State
12	MAPOLY	State
13	NOUN	Federal
14	OGITECH	State
15	OOU	State
16	Osun State Polytechnic, Iree	State
17	Oyo State College of Health Sciences and Technology	State
18	UATM GasaFormation	Private
19	University of Ibadan	Federal
20	Unilag	Federal
21	Unilorin	Federal
22	TASUED	State

Section 2: Cyber-Crime Issues and Solutions

The following were considered under the subsections previously discussed causes of cyber-attacks on institution web portals:

A. Personal Device Usage

All respondents confirmed that institutions allow the usage of personal devices in the school, which are not only used for teaching and learning but for other social functions as well. The table below gives detailed information from respondents.

Table 2: Personal Device Usage Statistics

S/N	Personal Device Usage	Frequency in Percentage	
1	Do you use personal devices for learning and teaching only?	Yes	39.4%
		No	60.6%
2	Do you use personal devices for both academic and non-academic activities?	Yes	98.5%

		No	1.5%
3	Do you have active security tools like antivirus, firewalls installed on all your personal devices?	Yes	59.1%
		Maybe	10.6%
		No	30.3%
4	Do you login into school portals with personal devices?	Yes	81.8%
		Maybe	1.5%
		No	16.7%

The porosity of the least of the personal devices used on the institutional portal is enough for cyber-attackers to perpetrate their acts and steal vital information with or without the knowledge of the user.

B. Institutional Data

Institutional data ranging from admission and registration to result processing are some of the data accessible to the clienteles at one point or the other. These information are most likely to be susceptible to attacks when the users gain access to the institutional portal.

Table 3: Institutional Data

SN	Institutional Data	Frequency in Percentage	
1	Is your institution using a single portal for all the services provided such as the website, staff and student information system, admission and payment, result processing?	Yes	53.0%
		Maybe	4.5%
		No	25.8%
		I don't know	16.7%
2	Do you know if your institution portal(s) is/are secured?	Yes	34.8%
		No	21.2%
		Maybe	43.9%
3	Approximately how much does your institution spend annually on cyber security products?	None	4.5%
		Less than $100 (₦30,000)	1.5%
		Over $200 (₦60,000)	1.5%
		Over $500 (₦150,000)	4.5%
		I don't know	87.9%

From the responses obtained from the survey, most schools make use of a single portal that provides centralised database for easy access and manipulation of data. As good as this may be, a single successful attack on any of these system can threaten the entire system and if no proper measures are put in place, can shut down the system. Also, the users of these system have little or no idea on the security state of the portals been used, hence the infiltration of attack through the user can also endanger the system.

C. Threats

From findings, a good number of the participants has no prior education of cyber threats, attacks and how to prevent them.

Table 4: Threats

SN	Threats	Frequency in percentage	
1	Have you had any education or information on cyber-crimes before?	Yes	43.5%
		No	46.4%
		Maybe	10.1%
2	Have you experienced cyber-attacks before on personal devices?	Yes	28.8%
		Maybe	6.1%
		No	65.2%
3	Has the security of your institution web portal being breached before?	Yes	25.8%
		No	30.3%
		Maybe	43.9%
4	How often does your institution web portal get breached?	Often	8.8%
		Rarely	58.8%
		Never	32.4%

D. Precautions

Table 5: Precautions

SN	Precautions	Frequency in Percentage	
1	Does your institution have concerns for cyber-crimes?	Yes	48.5%
		Maybe	34.8%
		No	16.7%
2	Have you ever gone through cyber security training in your institution before?	Yes	80.3%
		No	19.7%
3	How often do you get trained on cyber security?	Never	51.5%
		Rarely	40.9%
		Often	7.6%

E. Solutions

To make the institution web portal a safe place and to fight cyber crime, what are the things the management of these institutions should research into?

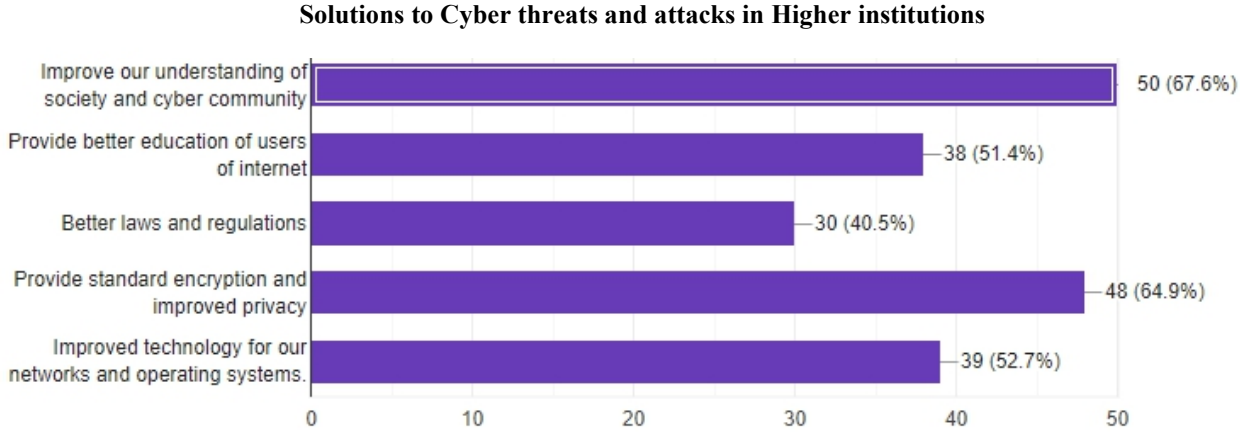

Figure 3: Possible solutions to combat cyber attack and threats

4. Conclusion

To a great extent, this study has revealed the lapses that occur within the higher institution environment on the part of the management of the school and the clienteles in combating cyber threats and attacks. To make up for the lapses, the points raised in proffering solutions should be critically looked into. Firstly, massive sensitization on cyber crimes and various ways of preventions should be given to users of these portals. Secondly, individual user should ensure that their devices are secured and less prone to attacks. Finally, institutions, in addition to what is obtainable at the moment, should provide multi-level security for their web portals and if possible decentralise some of the systems to avoid collateral damage.

References

Carlos Soto. (2016). Data Breach 101: Cyber Security Issues in Higher Education - Blog | Tenable Network Security. Retrieved February 15, 2017, from https://www.tenable.com/blog/data-breach-101-cyber-security-issues-in-higher-education

EDUCASE. (2018). Elevating cybersecurity on the higher education leadership agenda Increasing executive fluency and engagement in cyber risk.

Punch. (2017). African universities battle hacking, cyber crimes.