MALAYSIAN JOURNAL OF APPLIED SCIENCES 2024, VOL 9(1): 1-9
E-ISSN:0127-9246 (ONLINE)
http://dx.doi.org/10.37231/myjas.2024.9.1.338
https://journal.unisza.edu.my/myjas

ORIGINAL ARTICLE

An Investigation Into the Awareness Level of Universıty Undergraduates on Cyber Incident Reporting and Respeonse in Kwara State

Oyelakin Akinyemi Moruff*[1]

[1]Department of Computer Science, Faculty of Natural and Applied Sciences, Al-Hikmah University, Ilorin 240281, Nigeria

*Corresponding author: amoyelakin@alhikmah.edu.ng

Received: 26/10/2023, Accepted: 29/04/2024, Available Online: 30/04/2024

Abstract

Despite the increasing use of computers and internet resources for various purposes in different sectors of the economy, threats and attacks in cyberspace are on the increase. This is because internet attackers keep devising new techniques to evade being detected. The attack types include denial of service attacks, financial theft, espionage, subversion and identify theft. Many Nigerian cyber user communities are exposed to online threats. Despite efforts by government and IT security stakeholders to check the menace of cybercrime among Nigerians, cyber safety is still being considered to be very low. This may be as a result of lack of holistic measures for reporting and tackling the menace of crime in the country. Preliminary investigations revealed that some of the technological, administrative and legislative measures put in place in Nigeria to tackle the menace of cyber security have not given adequate attention to cyber incident reporting and response. This study used a structured questionnaire to source for the opinions of some University undergraduates in Kwara State, Nigeria. The questionnaire was used to investigate the level of awareness of the selected students about cyber incident reporting and response. The target population have ages that fall in youthful bracket and they are considered to youths who use internet resources for various purposes. The responses of the respondents were analysed using descriptive statistics. Statistical results revealed that larger number of students investigated is well aware of cyber incident reporting and response. Then, suggestions were made on how to achieve holistic strategy that can be used for promoting incident reporting and response among internet stakeholders in the country. It is argued that such measures will facilitate proactive means for tackling increasing cyber threats in the country.

Keywords: Cyber Safety, Cyber Incident Reporting, Cyber Security Awareness, Internet Threats

Introduction

The sophistication of attack campaigns in cyberspace increasing daily (Omodunbi, Odiase, Olaniyan and Esan, 2016; Nigerian Communications Weekly, 2017). Statistics from Forbe as argued by (Morgan, 2015) showed that cyber-attacks cost businesses as much as USD400 to

USD500 billion a year excluding the cost of unreported cases. Nigeria is among the countries that suffer from these cyber threats. SeveralAs Africa's digital infrastructure and Internet user base grows, the need to coordinate and manage Internet growth and development becomes increasingly important (Towela & Tesfaye, 2015). According to National Crime Prevention Council (2012), cybercrime is defined as any criminal activity involving computers and networks, which can include financial fraud, malware infection, insider abuse, denial of service attacks, cyber stalking and cyber scams. Yh5nudgxThe Nigeria Cyber security Outlook is very challenging as more cyber threats are reported in the country in recent terms (Deloitte, 2018; Nigerian Communications Weekly, 2017; Symantec, 2016, 2017, 2018). Deloitte (2018) stressed that year 2017 recorded more cyber incidents in Nigeria as there was a swift rise in several cyber Ponzi schemes (that is, schemes that promised unbelievable financial returns on investment). These schemes duped a good number of Nigerians by disappearing months later. Another very monumental cyber-attacks reported in Nigeria during the 2017 year was Wannacry ransomware that targeted many systems in about 150 worldwide (Deloitte, 2018).

As part of the efforts to reduce cybercrimes, the Nigeria Cyber Security Project was established during the regime of former President Olusegun Obasanjo as an initiative to secure the Internet for Economic Development and Growth (Tyendezwa, n.d.). Symantec, in its 2018 report, argued that attackers are becoming more innovative, organised and sophisticated, so much so that they are efficient in uncovering new vulnerabilities and escaping detection. Aladenusi (2017) argued that cyber-attacks would continue to grow and only the informed and prepared would survive with minimal losses. As reported in a cyber-security survey of Nigeria (Serianu, 2016), 97% of the respondents were very concerned about cyber security issues, indicating the impact the threats have created among Nigerian online communities.

Efforts by Nigerian government authorities concerning Internet threat prevention and protection are vast. However, there is need for improvement on the area of incident reporting and response. For this reason, it is essential for government regulatory agencies and other IT stakeholders to educate the internet users more. In the current arrangement, as set out in the Nigerian Cybercrimes Act 2015, the Office of the National Security Adviser is in charge of the administration and enforcement of measures to counter cyber related crimes.

According to the UK Cyber Security Strategy (2011), the UK seeking to tackle cybercrime against its citizens through a number of innovative and responsive measures. Some of the approaches include but not limited to: reducing online vulnerability, restricting criminal activity online, increasing awareness and visibility of threats among its citizens, improving incident response, fostering a culture that manages online risks. Nigeria can borrow a lot from these innovative approaches. There is US-CERT (United States Computer Emergency Readiness Team) which collaborates with other government agencies in the area of incident reporting and response in United State of America. The agency provides adequate technical support, investigation, analysis to every internet security breach that occurred and reported.

Internet governance and security follows a multi-stakeholder model in many countries (references) and Nigeria can only achieve improvement in its effort to make cyber space safer by following this model. As a nation, Nigeria requires a better understanding of the society, cyber community, improved government policies and the right internet culture (Serianu, 2016; Deloitte, 2017). This article provides overview of measures that can be used to improve strategic cyber incident reporting and response in Nigeria.

The 2017 report provided by Serianu gave cyber security information about Nigeria and some other African countries. The report uncovered and explained the top threat trends that are impacting regional organizations, businesses and private individuals. It was equally gathered in Serianu (2016) that most Nigerian organisations are ill-equipped to respond to information security threats and this make response to be far from being achieved. The paper suggested that public and private organisations within the country should rethink and rework their whole approach to information security practices. However, the trends in online attacks demand that joint measures

are taken over time. To be able to apply countermeasures effectively against all forms of cyber threats in Nigeria, a practically-oriented strategy that can strike a middle course between technical and non-technical needs will be required. For instance, there is a need to build cyber intelligence measures where government and other ICT stakeholders in the country can jointly handle reported cyber-related issues (technical, administrative, legal). Situational awareness for the internet users should be improved upon by the stakeholders as advocated by Serianu (2016). This study seeks to investigate the level of awareness of selected university undergraduates in Kwara state concerning cyber incident reporting and response.

The internet is an information infrastructure that serves many useful purposes for governments, businesses, industries and individuals. Despite some of the benefits of the internet, people with malicious intent use malware such as viruses, botnets, trojan horses to launch attacks in the internet (Son & Mohammed, 2012; Seenivasan & Shanthi, 2014). Nigerian government released Nigerian cybercrime act in 2015. The Act clearly helps in securing the internet space better. Cyber incidents can have serious consequences for individuals and business organisations when occur. Cyber security incident management involves a cycle that consists of preparation, detection, incident containment, mitigation and recovery. For this reason, the way cyber incident is reported and responded to matters a lot. Despite many studies on cyber security issues in Nigeria, there is less focus on incident reporting and response culture among Nigerian internet public. Thus, this study seeks to investigate the level of awareness of selected university undergraduates in Kwara State regarding internet incident reporting and response. It is believed that this approach will provide additional insights on the level of know-how of Nigerian internet public regarding cyber incident reporting and response.

Related Studies

Omodunbi, Odiase, Olaniyan and Esan (2016) carried out an analysis on cybercrimes in Nigeria. The authors provided some notable guidelines on detection and prevention strategies that can be used to check cyber security issues in the country. The emphasis of the work was to evaluate the level of involvement of some Nigerian students in cybercrime and to determine their vulnerability in such crimes. Frank and Odunayo (2013) in their paper defined the concept of cybercrime, identified the reasons for cyber-crime and its eradication. The study investigated he managers of cyber security in Nigeria and the reasons for their involvement. It furthered discussed the methods of stepping up cyber security in the country and then made recommendations that would help in checking the increasing rate of cyber-crimes that were highlighted. The paper also discussed some challenges of cybercrime and present practical and logical solutions to these threats.

Ajiji (2017) reported an overview of Cybercrime and Cyber-security in his work. The author defined the concept of cybercrime; identify reasons for cyber-crime and its eradication. The study looked at those involved in the development of cyber security strategy and the reasons for their involvement. Methods of stepping up cyber security and the recommendations that would help in checking the increasing rate of cyber-crimes were highlighted. The paper also attempts to name some challenges of cybercrime and present practical and logical solutions to these threats.

Towela and Tesfaye (2015) identified the factors that are responsible for the poor implementation of national ICT policies and strategies in Africa and its resultant effects in causing cyber-related issues. The study pointed to the fact the capacity gaps caused by this development cause security threats.

Osho and Onoja (2015) carried out a qualitative analysis of the current Nigerian National Cyber Security Policy and Strategy documents. The authors analysed the documents in the light of selected harmonized strategy developmental frameworks and subsequently comparatively evaluated with similar documents of selected countries. After the analysis, the national documents were found to have met majority of the requirements in terms of content, but failed to address certain elements of concern to cyber security in the Nigerian environment.

According to the Nigeria Cyber Security Policy of 2014, five key cyber security threats have been identified and they were listed as posing significant challenges to Nigeria. These include: Cybercrime, Cyber-espionage, Cyber conflict, Cyber-Terrorism and Child Online Abuse & Exploitation. Ojeka, Ben, and Ekpe (2017) carried out an appraisal of audit committee effectiveness concerning cyber security in the Nigerian banking sector. The emphasis of the work was to determine how cyber safety is promoted in the Nigerian banking sector.

Moreover, as part of efforts to stem a particular cyber threat called Cyber bullying, Cyber Angels (2007) provided several safety tips on measures that parents should put in place to protect their children while online. The study provided cyber situational information to parents in order to protect their children against cyber bullying. The recent Nigeria Cyber Crime Prohibition and Prevention Act published by Nigerian government is a welcome development but future review should not be delayed as situation warrants threats keep evolving. The act provides an effective, unified, and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrime in Nigeria FGN (2015). The act needs to include other framework such as technical and administrative efforts to stem some of the internet crimes.

Australia Communication and Media Authority (2010) identified that the assistance of various degrees that were provided to target audiences particularly children in the age brackets from four to seventeen, on how to manage online risks so that their experiences are safe and positive were investigated. National Cyber Security Alliance (2016) provided cyber security information for online users. The importance of the work is for a victim of attack to report appropriately in good time. This gives internet victim a chance to recoup any losses and ensure that the attackers are brought to justice.

Methodology

This study used descriptive statistics to represent the opinions of selected university undergraduates in four higher institutions in Kwara State, Nigeria. The research instrument was a questionnaire. It was administered to obtain vital information from the target audience. The pieces of information were used to ascertain the level of awareness of the respondents concerning cyber incident reporting. Then, the empirical evidence obtained was used to make some suggestions on how to arrive at improved and holistic internet reporting and response strategy in the country.

Data Analysis

The first stage in methodology used is data collection. The collected was used to investigate the level of awareness of respondents on incident reposting and response in the state used as a case study. The data gathered were analysed using Microsoft Excel software. In this study, a total of 450 questionnaires were administered among selected undergraduates in four higher institutions located in Kwara State, Nigeria. The study used simple statistics to analyse the responses provided by the respondents. 446 questionnaires that were properly filled were retrieved and used for the analysis. The results of the data analysis are captured in frequency distribution involving percentage and basic mean computation

Results and Discussion

Results of Data Analysis. As shown in Table 1, out of all the respondents used for the study, 64.8 % of them are males while 35.2 % are females. This is a demonstration that there are more male students used in the study compared to the female ones.

Table 1. Respondents' Gender Distribution

Gender	Frequency	Percentage (%)
Male	289	64.8
Female	157	35.2
Total	**446**	**100**

Source: Researcher's Field Survey, 2021

The distribution of the respondents according to their level is as shown in Table 2. From the results obtained, it is evident that students in 400 level are the largest population as respondents.

Table 2. Respondents' Class Distribution

Class	Frequency	Percentage (%)
100l	51	11.4
200l	115	25.8
300l	128	28.7
400l	137	30.7
Above 400l	15	3.4
Total	**446**	**100**

Source: Researcher's Field Survey, 2021

The results obtained in table 3 was for the evaluation of the level of awareness of the sampled university undergraduates in Kwara State on internet reporting and response. The grand mean for all the responses were obtained to be 3.89. Based on the values obtained for the mean and the Grand Mean, it can be deduced that majority of the Nigerian undergraduates sampled are of the opinion that the level of awareness of the students on cyber incident and response in the state is above average.

Table 3. Level of awareness of Nigerian undergraduates on cyber incident reporting and response

S/N	STATEMENT	SA	A	D	SD	Mean
1	Internet public in Nigeria do not have well structure incident reporting platforms	388	45	7	6	3.970852
2	I am well aware of need to report cyber incident to appropriate authority is it occurs	403	24	14	5	4.089686

3	The authorities in charge of cyber incident in Nigeria are well known and are doing their jobs	287	158	3	3	3.67713
4	Social sites such as facebook, twitter have exposed many Nigerian youths to cyber related threats, and/or offences	376	57	10	3	3.890135
5	Cyber response is very low in Nigeria	388	45	11	2	3.881166
6	Privacy concerns have reduced interest in reporting cyber incidents to authorized bodies	421	22	3	0	3.923767
7	Lack of coordinated cyber incident reporting strategy is response for low response in tackling cybercrimes in Nigeria	408	36	1	1	3.923767
8	It is not always safe to report cyber bullying, internet fraud, hacking attempt e,t,c to regulatory agencies on time	389	51	5	1	3.85426
9	There is no coordinated efforts for cyber incident reporting and response in Nigeria?	358	98	6	3	3.950673
10	If holistic measures by government agencies and IT security stakeholders are put in place cyber incidents will reduce in Nigeria	358	75	11	2	3.813901

Source: Researcher's Field Survey, 2021

Suggested Measures to achieve Improved Cyber Incident and Reporting Strategy Based on the feedbacks from the respondents in Kwara State and the current arrangement for tackling cyber security issues in Nigeria, holistic measures for handling cyber incident reporting and response are suggested in this study. It is suggested that there is a need to integrate technical and non-technical information security efforts among different stakeholders. Having holistic approach in place will eliminate the technological, legal and institutional barriers that can hinder collaborative information exchange against cyber threats. Figure 1 shows the processes that such holistic cyber incident reporting and response can follow.

The summary of the general strategies that can be used for handling cyber incident reporting and response in the country is depicted in figure 1. It is expected that such efforts should be holistic enough so as to cover all aspects that will attend to cyber-criminal cases from the start to the end. Such approach will fasten investigation, arrest, prosecution and conclusion of cyber-related cases, early enough than it is currently obtained.

It is believed that the holistic approach will enable government authorities, agencies, IT researchers, several private IT security stakeholders to achieve an improved Cyber incident reporting and response. Members of the strategic team can be well drawn from relevant government agencies and private IT stakeholders like Cybercrime Working Group (NCWG), EFCC, NITDA, NCC, law enforcement agencies, NIRA, ATCON, Security experts in academia and other stakeholders in the Nigerian IT industry, legal practitioners and so on.

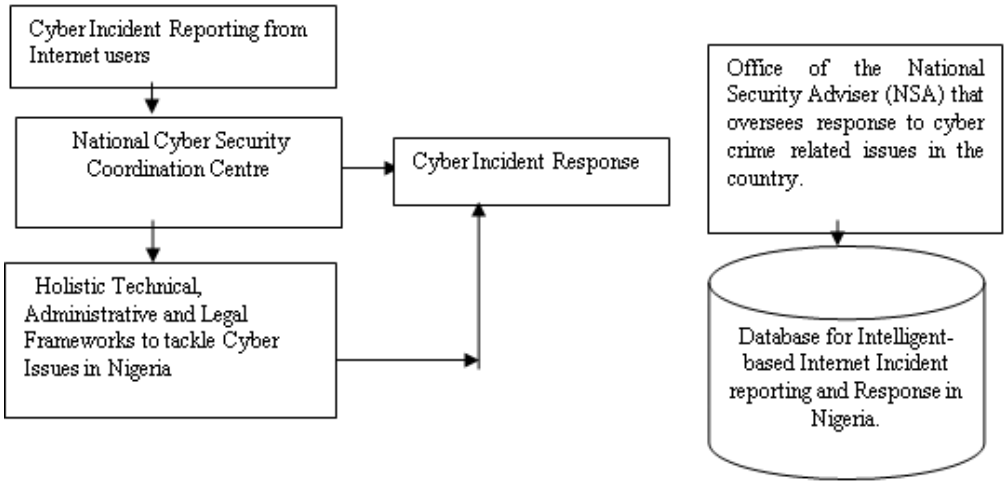

Figure 1. Suggested Holistic Strategy for Improving Nigerian Cyber Incident Reporting and Response

Statistical evidence showed that the level of awareness about cyber incident reporting and response among the selected university undergraduates in Kwara State, Nigeria is high. Moreover, it is evident that majority of the respondents indicated that culture for cyber incident reporting and response is above average in the state. One of the factors attributed to this negative development is called privacy concern. Culnan and Armstrong (1999) argued that consumers have two kinds of privacy concerns in the internet space. First, they are concerned over unauthorized access to personal data because of security breaches or the lack of internal controls. Secondly, they are worried about the risk of secondary use without their consent. The opinions gathered from respondents confirmed the privacy concerns.

The statistics obtained from the responses were used as the basis to suggest to some measures that are considered to be holistic for internet reporting and response strategy. For the Incident Reporting and response Strategy to work better in Kwara State and Nigeria as a whole, government agencies and private IT security stakeholders should try to ensure that when a cyber-incident occurs and reported, the response should be coordinated and holistic in nature such that the victims will feel secure technically, legally and so on. While investigating an incident, caution should be made not to divulge the information of the reporting individual, group or body. In the proposed Strategic Internet Incident Reporting Scheme, privacy is expected to be handled with very great caution because of the legal implications.

Conclusion

This study investigated the level of awareness of a number of University undergraduates in Kwara State, Nigeria on cyber incident reporting and response. The results of the statistical analysis showed that there is some level of awareness on cyber incident reporting and response among the selected undergraduates. Then, some suggestions were made with a view to achieving improved cyber incident reporting and response among IT stakeholders in Nigeria. It was argued that some of the suggested measures will help improve security measures among all internet stakeholders. It is equally pointed out that the measures need to be holistic such that cyber security research, investigation, analysis, technical support and prevention of security breaches can be improved upon in the country.

These suggestions are based on the understanding that no single cyber framework by a government agency or individual can be adequate to provide all-in-one intelligence for fighting online threats. Such efforts will aid in the detection of internet-crime related crimes, gathering of cyber security intelligence as well facilitate timely response to the threats. Thus, this study can be argued to have provided additional insights on how Nigerian cyber space can be protected better through situational awareness.

References

Ajiji, Y. M. (2019). Cyber Security Issues in Nigeria and Challenges, International Journal of Advanced Research in Cyber Security Issues in Nigeria and Challenges. (October). https://doi.org/10.23956/ijarcsse/V6I12/01204

Aladenusi Tope (2017) Nigeria Cyber security Outlook retrieved from http://blog.deloitte.com.ng/wp-content/uploads/2017/01/Cybersecurity-Outlook-2017-by-Tope-Aladenusi.pdf

Australia Communication and Media Authority (2010): Connecting Parents to Cyber Safety Resources

Central Bank of Nigeria (2003): Report of the Technical Committee on Electronic Banking, retrieved from https://www.cbn.gov.ng/OUT/PUBLICATIONS/BSD/2003/E-BANKINGRPT.PDF

Culnan M.J. and Armstrong P.K. (1999): Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Emperical Investigation, Organisation Science, 10(1): Jan-Feb 1999

Culnan M.J (2000): Protecting Privacy Online: Is self-Regulation working? Journal of Public Policy and Marketing, 19 (1): 20-26

Cyber Angels (2007): Cyber Safety Guide http://www.cyberangels.org/docs/cybersafetyguide.pdf retrieved on Jan 5, 2016.

Deloitte (2018).2018 Nigeria Cyber security outlook retrieved from https://www2.deloitte.com/ng/en/pages/risk/articles/2018_nigeria_cybersecurity_outlook.html

Fayomi, O., Ndubisi, O. N., Ayo, C., Chidozie, F., & Ajayi, Lady. (2013). Cyber-Attack as a Menace to Effective Governance in Nigeria. 107–116.

Federal Government of Nigeria (2015). Nigeria Cyber Crime Prohibition and Prevention Act

Federal Republic of Nigeria (2019). National security strategy. December, 2019.

Frank and Odunayo (2013). Approach to Cyber Security Issues in Nigeria: Challenges and Solution, IJCRSEE) International Journal of Cognitive Research in science, engineering and education 1(1)

ISACA (2011): Mobile Payments; Risks, Security and Assurance Issues, retrieved from https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpmp

Morgan, S. (2015). The Business of Cybersecurity: 2015 Market Size, Cyber Crime, Employment, and Industry Statistics, retrieved from https://www.forbes.com/sites/stevemorgan/2015/10/16/the-business-of-cybersecurity-2015-market-size-cyber-crime-employment-and-industry-statistics/#659a87e95d0d

National Crime Prevention Council (2012): Cybercrimes retrieved from www.ncpc.org/resources/files/pdf/.../13020-Cybercrimes-revSPR.pdf on Jan 13, 2016

National Institute of Standards and Technology, (2012) US Department of Commerce, Special Publications, Revision 2 Draft 1

National Cyber Security Alliance (2016). Stay Safe |Online retrieved from https://staysafeonline.org/business-safe-online/report-cyber-attacks/ retrieved on January 8, 2016

Nigerian Communications Week (2017). Cyber Attack Trends: Mid-Year Report retrieved from https://nigeriacommunicationsweek.com.ng/cyber-attack-trends-mid-year-report/ on 3rd July 2018

Omodunbi, B. A., Odiase, P. O., Olaniyan, O. M., & Esan, A. O. (2016). Cybercrimes in Nigeria: Analysis, Detection and Prevention. FUOYE Journal of Engineering and Technology, 1(1).

Osho, O., & Onoja, A. D. (2015). National Cyber Security Policy and Strategy of Nigeria : A Qualitative Analysis. International Journal of Cyber Criminology (IJCC)9(June), 120–143. https://doi.org/10.5281/zenodo.22390

Ojeka, S. A., Ben Caleb, E., & Ekpe, E. I. (2017). Cyber Security in the Nigerian Banking Sector : An Appraisal of Audit Committee Effectiveness, 7(2), 340–346.

Serianu (2016). Africa Cyber Security Report, retrieved from https://www.serianu.com/downloads/NigeriaCyberSecurityReport2016.pdf

Serianu (2017). Demystifying Africa's Cyber Security Poverty Line, Africa Cyber security Report. retrieved from http://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf

Symantec (2017),Internet Security Threat Report volume 22 retrieved from https://www.websecurity.symantec.com/security-topics/istr-2017-infographic

Symantec (2018). Internet Security Threat Report volume 23 retrieved from https://www.symantec.com/.../symantec/docs/reports/istr-23-executive-summary-en.pd. on Aug 20, 2018

UK Government (2011). The UK Cyber Security Strategy, Protecting and promoting the UK in Digital World, retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

Tyendezwa T. George-Maria (n.d.). Legislation on Cyber Crime in Nigeria: Imperatives and Challenges, retrieved from https://docplayer.net/7834091-Legislation-on-cybercrime-in-nigeria-imperatives-and-challenges.html

Tyendezwa T. George-Maria (2016). Cybercrime Investigations and Prosecutions: Bridging the Gaps, 26th National Conference of Nigeria Computer Society, Abuja, retrieved from http://www.ncs.org.ng/wp-content/uploads/2016/07/Cybercrime-Investigations-and-Prosecution-Bridging-the-Gaps.pdf

Towela Nyirenda-Jere and Tesfaye Biru (2015): Internet Development and Internet Governance in Africa

How to cite this paper:
Moruff, O. A. (2024). An Investıgatıon into the Awareness Level of Universıty Undergraduates on Cyber Incident Reporting and Response in Kwara State. *Malaysian Journal of Applied Sciences, 9(*1), 1-9.