Sub-Sahara African Academic Research Publications
September, 2023 Editions

JAAS
Journal of African Advancement & Sus. Studies
Vol.29, No.2, ISSN: 3125-5521

CYBER-SECURITY: PROSPECTS AND CHALLENGES FOR DEVELOPMENT IN NIGERIA.

[1]OLAITAN, OLUMIDE OLATUNDE; [2]AZEEZ, LUKMAN ADEDAYO; [3]ADENIRAN, EMMANUEL GBADEBO; [4]IGE, MICHAEL ADEKUNLE

[1&2]Accountancy Department of Accountancy, the Oke-Ogun Polytechnic, Saki. [3&4]Department Banking & Finance, the Oke-Ogun Polytechnic, Saki.

Abstract

Cybercrime has become so rampart in information technology and this pose a great challenge to the economic development of the nation. Cybercrime is the series of organized activities which pose a threat to the users, cyber space and cyber security. This study therefore examined the cyber security, prospect and challenges for development in Nigeria with a case study of Oyo State and also investigates the effect of cybercrime on economic development in Nigeria using the same case study. The study used survey research design using quantitative data gathered via questionnaires administered to selected 150 cyber operators in Oyo State. The data was analyzed using regression analysis. The study revealed that cybercrime has negative impact on the economic development of the nation. It is therefore recommended that adequate security measures should be adopted by the Nation through relevant agencies to curb the incessant cybercrime in the cyberspace.

Keywords: Cyber Security, Cyber-crime, Information Technology, Economic Development, Cyberspace.

Introduction

Cybercrime has become an emerging issue for governments, entities and individuals and how to guide against it has posed biggest challenges to its users. Its security has also becoming major obstacles across the globe **which grows at a faster rate. Guiding against this menace is a major challenge to modern world; which brought about customers fear in this modern technology. Protecting information nowadays has becoming critical issues**. Anytime we discussed about cyber security our main attention will be on 'cyber crimes' which are rampart on daily basis. More so, it has resulted into unpalatable situations like unlawful issues, sending of mails, internet crimes, ATM fraudster and a lot of miscreants to have access for their unpleasant acts (Olumide and Victor, 2010).

In recent times, cyber-crime has been on alarming rate which has adverse effect on the socio-economy of the country. Two decades ago, immoral cyberspace users had been using the internet to engage in series of crime; this resulted into mixed feeling and fear to the general populace alongside with personal security. This has led to unexpected experiences nowadays and it has required urgent attention by putting in place legislation that would protect all stakeholders in cyber space.

Roseline, (2012), opined that Nigerian cyber criminals are inventing or engaging in new ideas on daily bases in perpetrating this act, in which the current ways of detecting this menace are now outdated to curb them.

Objective of the study

This study seeks to examine the cyber security, prospect and challenges for development in Nigeria and to investigate the effect of cybercrime on economic development in Nigeria.

Literature review

Conceptual clarification

Concept of cyberspace, cybercrime and cybersecurity

As information technology advances, the meaning of cyberspace, cyber security and cybercrimes also improved.

Cyberspace: Cyber-space refers to as an endless space which has changed the ways we pass information, run appliances at various homes and administer governance. It is also known as series of network that depends on each other which gives supports to technology.

Cybersecurity: According to (CYBERPEDIA, 2017) cyber security is a ways adopted in preventing the quality and worthiness of information from illegal users.

Privacy, adequate, effective and prevention of information is the paramount steps to be taken by firm/users in adopting necessary measure. Globally, many people are currently living in a digital world or a cyber-form. Internet facilities have becoming an avenue for users to communicate with to friends and family. Cyber-security are series of scientific knowledge, ideas and practices put together to guide against networks, computers, set of instructions and data from being tampered with, damaged by unauthorized users. Cyber-security is the procedures and regulations adopted in securing cyber space.

The International Telecommunications Union's (ITU's, 2008) defined cyber security as "interconnected components (policies, security concepts, enabling legislation and technologies devices) adopted in securing users assets and its environment at large.

Oliver, (2010) opined that, cyber-protection entails joint efforts from both the users and the system. Problems created by breaches in our cyber-security are developing at alarming rate and adequate measure must be put in place to check the menace. (Adebusuyi, 2008).

Cybercrime: Cybercrime is a term for any illegal activity that takes place through the use of an internet. Department of Justice in United State defined cybercrime any unlawful acts that is perpetrated through the use of internet. It also refers to as the series of created crimes affecting cyber village and its security. Globally, cyber syndicates had pose a high threat to our economy and national development. It also means illegal activities perpetrated using computers and the Internet, both monetary and non-monetary offences such as having access to accounts of millions of people through online banking, creating and distributing viruses on other computers and stealing personal information from other users.

Cyber-crime as defined by (Laura,1995) as "A criminal activity involving an information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or

suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud". In a lay man's understanding cybercrime may be refers to as unlawful access in perpetrating to personal information of uses through computer and internet facilities.

Aim of Cybersecurity

The following are the purpose of cybersecurity as sited by (Nikhita Reddy and Ugander Reddy, 2013) and (Yakubu, 2017) as follows:

- Assist in reducing the attack on users Information.
- It encourages all stakeholders to inculcate the habit of cyber security.
- In ensuring that there is collaboration with all cyber users to guide against cyber world.
- In serving as a guard against quality and trustworthiness of interconnected devices and illegal users.
- To assist in having knowledge on the new ideas spring up in cybercrime and come up with proactive measures.
- To enhance confidentiality on cyberspace.

Trends changing in cyber security

The following are the trends that affect cyber security as sited by (Nikhita Reddy and Ugander Reddy, 2013).

Web servers: Threatening of having unauthorized access to information on internet and spreading malicious code is on the high side. Cyber syndicates perpetrate these illegal acts through some legitimate web servers that has compromised. Even, most of the attacks get the attention of media, is a great bottle neck. Nowadays, proper attention should be put in place to secure web servers and its applications. Internets are best avenue for cyber criminals to perpetrate their deal. Therefore, safer browser should be adopted when important transaction is taken place in order not to be a victim of the fraudster.

Cloud and its services: Nowadays most entities (small, medium and large) are gradually embracing cloud services. In short, entities globally are gradually embracing the clouds. These current happenings posed a huge obstacle for cyber security globally. Cloud services needs to upgrade gradually in order to avert losing valuable information.

Advanced Persistent Threat: This is a newly approach adopted to take care of cybercrime ware. In years' back, web filtering or IPS have played a major role in preventing such attacks. As attackers develop and employ vaguer methods, internet securities must collaborate with each other in order to detect and finding lasting solution to the attacks. Hence there is need to improve the security network in order to avert subsequent threats in the future.

Mobile networks: Nowadays, there is interconnectivity between each other globally. Protection of interconnectivity is a major issue. Most of the measures put in place to protect it are porous and many people using various devices such as personal computer, hand set etc. also required additional means of protecting their devices apart from the inbuilt security applications. Based on this, adequate measures should be adopted in securing the interconnectivity against this unlawful act on internet

Encryption: Encryption is a special code used to prevent information from looking at without authorization so that unauthorized person would not be able to read it. By encryption, the information will be converted using encryption key into unreadable cipher text. This technique is being used to protect data or information in transit through interconnectivity.

Role of social media in cyber security

The way we connected to the world socially has been on an increasing rate, companies and individuals must adopt new techniques to protect their personal information. Social media contributes immensely to cyber insecurity and has pose series of problems to users. Introduction of social among personnel is on the high side and it has become a bottleneck. Since this avenue are being used by most of this perpetrators daily, it has becoming a huge avenue for internet fraudsters to get access to private information and do away with valuable data. Hence, organizations/individuals should embark on proactive measures in preventing social media so as to avert loss of information/data.

Though, the power to disseminate vital commercial information are given to some people but care must be taken in given such power to those who are going to spread false information which might resulted in damaging their reputation. Even though interconnectivity is used to perpetrate crime, most entities cannot do without this e-communication because it plays vital roles in publicize their goods/products. Instead, adequate measure should be put in place to avert or notify them of the threat before the damage was done.

Types of cybercrime most prevalence in Nigeria

Hacking: This is an act of capitalizing on the shortcoming or loop holes in sets of programs to damage information and do away with vital documents from user's computer. Fraudster's through the use of software package gets password to gain access to information and at times, they may monitor what you do on your computer and thereby importing files from it. A hacker may also install programs to your system without your consent which will enable them to do away with personal belongings e.g. passwords, credit card information.

Cyber-theft: Cyber-theft is an act of gaining access into cyberspace through the use of computers and internet systems. Hackers break into the systems of banks and transfer money into their own bank account. Credit card crime is so rampart and most entities and money deposit banks did not expose this because their customers/investors might lose confident in them, **Spamming:** This involves sending mails and promotes advertising products on internet. It is becoming a major problem amongst entities, due to its overhead cost, not only in regards to bandwidth consumption but also to the amount of time spent in eliminating spam mail. Spammers are also introducing new approaches to avert spam filters, apart from imagery and permutation of the emails which cannot be discovered by spam filters.

Cyber harassment: This is intentional or electronically means of threatening an individual's such acts include cyber-stalking.

Cyber laundering: This is an illegal act through which funds is being transferred electronically so as to hide its source and possibly its destination.

Salami Technique: Salami is an economic scams or an opportunity to gain an advantage on confidentiality by gathering detail information.

Cyber terrorism: Cyber terrorism is a sponsored attack or political planned against information, interconnectivity, software programs which erupted into violence. (searchsecuriy.echtarget.com)

Cyber security techniques

Nikhita Reddy and Ugander Reddy,(2013) in his study highlight some techniques of cybersecurity as follows:

Access control and the use of password: Password and user name is the major key to secure our information and it should be the first steps to be taking as regarding cyber security.
Data Authentication: The origination of information received should be verified, authenticated before access i.e. it source should be reliable and trusted. Anti – virus software could be installed into the system in order to secure system from unwanted viruses.
Malware scanners: This is a means of scanning information and official papers that appears in a system so as to avoid harmful viruses or malicious code.
Firewalls: This is a software package that is being installed in a system to prevent hacker, unauthorized users to penetrate into our system through internet. Firewall used to verify the inflows and outflows of messages that pass through the internet and blocks unverified messages that do not meet the specified security criteria.
Anti-virus software: This is software package that use to prevent and protect tackle unwanted malicious programs in the system, such as worms. This software package is very essential and necessary for systems.

Challenges of cyber security in Nigeria
There are lots of problems facing cyber security in Nigeria some of which are:

1. There is no adequate cyber security to prevent and maintain interconnectivity and information issue.
2. Lack of expertize as regard cyber prevention and failure to pay attention or supervise and prevent national network, leading Nigerian and other African countries the top most internet criminal's and incidence of interconnectivity terrorisms.
3. Lack of required cyber legislation to bailed cybercrime.
4. Limited awareness of information communication technology(ICT) – the level awareness on ICT security are not enough on the part of enforcement agencies, those who regulate ICT, users and the likes.
5. There is need to develop and maintain an information society that respects values, rights/freedoms and assures same access to information, introduction of real understanding should be put in place to ensure adequate and sincerity in the use of ICTs in Nigeria. (United Nations Economic Commission for Africa, 2014).

Effects of cyber crime
Financial deficit: Cyber perpetrators are more or less a terrorists and their activity imposes much costs on individuals or society at large.
Loss in reputation: Entities had been reported of various scams which resulted into loss of huge of funds and loss of reputation and customers losing credibility in them.
Reduction in productivity: In an attempt to curb cyber criminality, companies productivity has reduced since informative and more attention are given on securing cyber criminality and unproductivity.

Remedies to cybercrime
Education: There is need to educate all stakeholders on how to maintain and update the security on their system when online. Corporations and organizations need to employ effective and efficient security management so as to safeguard their information.
Introduction software packages and Information Technology seminars for youths: Unemployment rate also emanated to increasing rate of e-crime in the country, government must provide employment opportunity for our young one and establish seminars for youths to show

case their potential. It will also be an avenue in development of information technology in the country.

Address verification system: This should be adopted in other to ascertain whether address provided on in the order corresponds with that of the billing statements.

Interactive voice response (IVR) terminals: These are current innovation or device that used to minimize fraud by collating "voice stamp" or "voice authorization" and authenticate whether it from customer before goods are shipped.

IP address tracking: This is a program used to monitor and check the IP address of orders whether is within the same country in which the billing and shipping comes from.

Adoption of video surveillance systems: The major bottleneck of this approach is that it concentrates mainly on human rights issues and legal advantages.

Antivirus and anti-spyware software: Antivirus graphics comprises of computer software which are design to highlight or to get rid of worms in computer and other unwanted software.

Firewalls: This is computer software that protects unauthorized access to the system. It can be hardware/software programs or both.

Cryptography: This is a scientific means of encoding and decoding information i.e. mailing information to other person using code that is understandable to the person that send and the receiver.

Cyber ethics and legislations: Cyber principles and legislations should be adopted and enacted to put an end to cyber-crimes. It should be a must for all stakeholders in cyberspace to abide to cyber ethics and legislations so that the rate of cyber-crimes will be drastically minimized. Service Providers must made available effective security measure to prevent their servers so as to prevent customers from falling victims of viruses and other set of instruction that control the operation of a computer. (Augustine, 2010)

Theoretical framework

The theory adopted in this paper is social theory.

Social theory: Security theories anchor on how to provide, implement and protect the society against failure and misused of information system. It was based ensuring security alert, motivation and training. (Kajava, 1979; Pipkin, 2000 and Proctor and Byrnes, 2002). Researchers theorised that user opinion on risks and choice is based on those views that can affect security system.This theory also explain causaion that policy makers should be properly adviced on behavioural problems that must put into cognisance as the time of formulaing plan of action in tackling internet criminalties within Nigeria.

Methodology

The method employed in this research was survey research design using quantitative data gathered via questionnaires administered to selected 150 cyber operators in Oyo State. The data was analyzed using regression analysis.

Finding and discussion

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.436[a]	.190	.131	.974

The model showed the Good fit Test. The adjusted R^2 showed that all explanatory variables could explain 13.1% of the dependent variables. This means that other variables which can predict economic development constitutes 86.9% and these were not captured in this study.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	30.645	10	3.065	3.231	.001[b]
	Residual	130.898	138	.949		
	Total	161.544	148			
a. Dependent Variable: Economic Development						

The table above showed the result of Analysis of Variance. The F value of 3.321with P-value of 0.001 (P< 0.05) indicates that all variables are jointly statistically significant to impact economic development in Ibadan Metropolis, Nigeria.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.536	.341		1.572	.118
	Cybercrime rate	.345	.090	.317	3.822	.000
	Fighting cybercrime	.015	.080	.015	.184	.854
	Level of investors	.187	.069	.219	2.726	.007
	Terrorism	.033	.063	.044	.521	.603
	Cyber security	-.018	.078	-.020	-.235	.814
	Enabling laws	.150	.079	.159	1.890	.061
	Vulnerability	-.084	.075	-.088	-1.108	.270
	Functional Cyber security	-.098	.084	-.107	-1.177	.241
	Cybercriminals are like terrorists	.014	.076	.016	.190	.850
	Preventive tools	.009	.072	.011	.130	.897
a. Dependent Variable: Cybercrime has any impact on economic development in Nigeria						

The coefficient table above established the relationship between economic development and cyber security variables. Rate of cybercrime has significant effect on Economic Development at β= 0.345, p<0.05(P-value of .000). Fight against cybercrime has positive and insignificant relationship with Economic Development of β = 0.15, p>0.05(P-value of .854). Cybercrime negative impact on Level of investors participation in Nigeria have positive and significant effect on economic development of β= 0.187, p<0.05 (P-value of .007). The study therefore established that rate of cybercrime and its effect on level of investors' participations in economic development significantly have effect on the economic development of the nation. Fight against cybercrime has negative and insignificant effect on economic development

Conclusion

The study examined the prospects and challenges of cyber security and its effect on Economic Development in Nigeria. The authors adopted survey research with sample size of selected 150 respondents within Oyo State. The study established that Cybercrimes affect level of participation

of investors in economic development; there is no holistic and pragmatic approach to fight against cybercrime. Cyber-security is also vulnerable to cybercrime.

Recommendations

The study therefore recommends that adequate security measures should be adopted by the Nation through relevant agencies to curb the incessant cybercrime in the cyberspace. There should be holistic and pragmatic approach to fight against cybercrimes in Nigeria. Cybercrimes should be declared as an act of terrorism. There is need to train and employed an ethical hacker in various firms and organization that connected to the internet.

Reference

Adebusuyi, A. (2008). the internet and energence of yahooboys sub-culture in Nigeria. *International Journal of cyber-criminolgy, 0794 - 2891, 2*(2), 368 -381.

Africa., U. N. (2014). Tackling the challenges of cybersecurity in Africa. *Policy Brief.NTIS/002/2014,Economic Commission for Africa.*

Augustine, C. O. (2010). Cybercrime and cert: Issues and probable policies for Nigeria. *DBI, Presentaion, November 1-2.*

Cohen,L & Felson, M. (1979). Social changes and crime rate trends: A routine activity approach. *American sociological review, 44*(4), pp. 588 -608.

Crocker, D. (1982). *standard for the format of ARPA internet text messages.*

CYBERPEDIA.(2017).What is Cybersecurity? Retrieved 1st August,2019 from http://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security.

Davis, R & Hutchison, S. (1997). *Computer crime in Canada.* Toronto: Thompson Canada Limited.

Felson, M & Clarke, R. V. (1998). *Oppurtunity makes the theif.* London: Police research series, policing and reducing crime unit, reseach development and statistics directorate. Retrieved from www.homeoffice.gov.uk/rds/prgpdfs/fprs98.pdf

Kajava, J. (1979). Effectively implemented information security awareness. An example from University Enviroment. *IFIP.TC 13th International conference on information security: Information security management the future.* Copenhagen,Demark.

Laura, A. (1995). Cyber crime and national security: The role of the penal and procedural law. *Research fellow, Nigeria institute of advanced legal studies.* Retrieved July 15, 2019, from http://nisls-nigeria.org/pub/lauraani.pdf

Longe, O. B ; Wada, F,; Anadi, A,;Jones, C, & Mbarika, V. (2010). A critical appraisal of the peel theory of community policing in age of cybercrime. *84th annual meeting, Louisiana State University.* Alexandra. Retrieved from http://www.laacademy.org/docs/schedule.pdf

Nikhita Reddy, G & Ugander Reddy, G. J. (2013). A study of cybers security challenges and its emerging trends on latest technologies. *International Journal of Scientific and Enginerring Research, 4*(9), 68 - 71.

Oliver, E. (2010). Cyber security holding. *Being lecture delivered at DBI/George Mason University conference, department of information management technology, federal University of tecnology , Owerri, 1-2 november,2010.* owerri.

Olumide, O.O & Victor, F.B. (2010). E-crime in Nigeria: Trends, tricks and treatment. *The Pacific Journal of Science and Technology., 11*, 50-62.

Pipkin, D. L. (2000). *IS security : Proctecting the global enterprise.* USA: Hewlett packard professional books. Prentice hall PTR, upper saddle river,USA.

Proctor, P. E & Byrnes, F. C. (2002). *The secured enterprise: Proctecting your information assets.* USA: Prentice hall PTR, upper saddle river, USA.

Roseline, O. M. O. (2012). Cyber capacity without cyber security: A case study of Nigeria's National policy for information technology (NPFIT). *The Journal of Philosophy, Science & Law., 12*. Retrieved July 15, 2019, from http://www.miami.edu/ethics/jpsl.

United Nation Economic Commission for Africa (2014). Tackling the challenges of cybersecurity in Africa. *Policy brief.NTIS/002/2014,Economic Commission for Africa.*

Yakubu, A. (2017). Cyber security issues in Nigeria and challenges. *International journal of advanced research in computer science and software engineering.*(7).

Ziff, D. (2015). Definition of computer security. encyclopedia. PCMag. Retrieved from http://whatis.techtarget.com/definition/cybersecurity