FEDPUKA JOURNAL OF SCIENCE, TECHNOLOGY AND CONTEMPORARY STUDIES
VOL 1 ISSUE 2, 2025

STRATEGIC AWARENESS OF CYBER-SECURITY IN COMBATING CYBER-CRIME IN NIGERIAN TVET ERA

NWANKODO, EMMANUEL NAZI
emmanazinwankodo@gamil.com
08037526059
DEPARTMENT OF PUBLIC ADMINISTRATION,
ABIA STATE POLYTECHNIC ABA,
ABIA STATE

OKEAGU CHARLES
DEPARTMENT OF PUBLIC ADMINISTRATION,
ABIA STATE POLYTECHNIC ABA,
ABIA STATE

ONICHAKWE CHARLES CHIMEZIE
charlesonichakwe25@gmail.com
charles.onichakwe@fedpolyukana.edu.ng
08038733240
DEPARTMENT OF GENERAL STUDIES
FEDERAL POLYTECHNIC, UKANA,
AKWA IBOM STATE

Abstract

The theme of this paper is Strategic Awareness of Cyber-Security in Combating Cyber-Crime in Nigerian TVET Era. This study examined the consequent effects of cyber attacks, threats, exposures and vulnerabilities in Nigerian economy. The methodology adopted for this study was a descriptive survey approach. Secondary data was used as a means of data collection. Findings of this study among others revealed that cyber-security technology and awareness is a vital tool and strategy to combat cyber attacks, threats, vulnerabilities and exposures. Based on the findings, the study concluded that cyber-security and aggressive awareness and attention is urgently needed in Nigeria and the world as there is growing trends of cyber-crime, threat and attacks in national economy of countries globally. Therefore, the researcher among others recommended that all hardware and software used by countries must be standardized in line with the set parameter and the Human Resource Department in organizations should be trained regularly to be abreast with the latest cyber attacking techniques.

KEYWORDS: ***Cyber -security, Strategy, Awareness, Cyber- Crime, Vulnerabilities***

Introduction

Cyber-attacks and crimes has been a new trend in the world as it negatively impacts on organization economically and disrupts the entire organization and business operations .It is gathered as a facts that ,cyber- crimes losses to organizations is about $300 billion to 1 trillion and to world economy total 0.4% to 1,4% of total GDP.

At present, there has not been any solution to cyber- attacks and threats but awareness and strategy implementation of policies is the best idea to this growing dastard trends

As organizations and national economy devices are interconnected with digital infrastructures, this increases cyber- attacks, hence, there is need for cyber-security in organizations and economy in all entirety.

The world is now digitalized and people are more technological savvy coupled with the growing trends of social media, and organizations compliant to the adoption of technology in their operations and activities

Also, as the world of organizations transits from conventional computing system to cyber system in terms of continued availability ,confidentiality and accuracy of information, hence, this led to several vulnerabilities of easy attacks and penetration to cyber systems due to lack of awareness and knowledge in this present 21st century technology and computing compliant.

Cyber-crimes could be experienced in the like of human factors level as a risk where paper based activities are used inconsistently. Also, officers in the organizational settings with sensitive and important information assets, if not trusted and honest could be a threats to the security of those vital assets of information within his reach.

The whole word and the economy is digitalized as a global phenomenon and development resulting to cyber- attacks and crimes in the area of information and data theft (WEF 2019).

Organizations and economy in countries of the world operates on the basis of new technologies for effectiveness and efficiency and this portend fast approach in preventing cyber- crimes and attacks as these criminals develop new measures every day in attacking public administration infrastructures, (Janczewski & Caelli, 2015).

International Telecommunication Union, (2018), posits that, organizations and individual user's property which include connecting computing devices, personal data, infrastructure, application servers, telecommunication systems and the summation of both stored and transmitted information in the cyber ecosystem.

Cyber security has been given a priority in global public and private organizations and economy as it was neglected then due to unawareness and poor co-ordination and attention given to cyber security as a result of poor network, poor cyber laws and inadequate skills ,knowledge as well as well - trained cyber security professionals in both public and private organizations (Adhikari ,2017).

Hence, quality security assist government and organizations in rendering effective, reliable and efficient services to the general public, ensure public and government relationship and communication and importantly, protecting sensitive and essential data as well safeguard the payment of ransom of money and public administration cyber space attacks, (Kapammbwe, 2011).

STATEMENT OF THE PROBLEM

Nations all over the world have become conscious of cyber-cyber threats. One thing is to be aware of a threat and another is to be conscious of it.

Cyber-crime has become a recurrent decimal in the national economy of nations all over the world. Countries are not leaving any stone unturned in combating the menace of cyber-crime in the society. This is as a result of the fact that huge assets belonging to countries globally have been lost because of the menace of cyber-crime. In Nigeria, several cases of cyber-crime have been reported in both the public and private sectors of the economy.

Cyber-crime, threats and attacks have affected the banking industry, manufacturing industry, agricultural industry, trade and investments etc. All these ugly development have impeded the growth and development of the Nation.

It is against this backdrop that the researcher decided to carry out this investigation so as to proffer solution to the problems.

OBJECTIVE OF THE STUDY

The specific objectives of this study is to:

i. Ascertain the meaning of cyber-security and cyber-crime

ii. Find out if cyber-security strategies and awareness are useful tools used in combating cyber-crime.

iii. Make useful recommendations on how to combat cyber-crime in Nigerian economy.

CONCEPTS OF SECURITY AND CYBER-CRIME

According to Olumide (2010), cyber-security is the practice of protecting internet connected systems such as hardware, software and data from cyber threat. It is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized system.

According to Strassman (2009) cyber-security is the collection of tools policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and users assets.

Cyber-security strives to ensure the attainment and maintenance of the security properties of the organization and users assets against relevant security risks in the cyber environment.

According to Schaeffer (2009) Cyber-security is the practice of protecting systems, networks and programme from digital attacks. These cyber attacks are usually aimed at accessing, changing or destroying sensitive information; extorting money from users via interrupting normal business processes.

According to Nayak (2013) cyber-crime is that group of activities made by the people by creating disturbance in the network, stealing others important and private data, document, hack bank details and accounts and transferring money to their own. Cyber-crime is defined as any criminal activity which takes place on or over the medium of computers or internet or other technology recognized by the Information Technology Act (Schaeffer, 2009). There are number of illegal activities which are committed over the internet by technically skilled criminals. Cyber-crime has become an uncontrollable evil in the society.

CYBER SECURITY STRATEGIC GOALS

According to Hooghe & Mark, (2002), the cyber security strategic goals lies on the following:

(i) Ensuring effectiveness and efficiency of infrastructures structures, processes in public sectors cyber-security.

(ii) Ensuring active international co-operation on cyber security

(iii) Co-operation with the private sector and other stakeholders

(iv) Engage in research and development in technologies by IT experts and universities for latest cyber –security technologies

(iv) Given support for education, awareness and information for the public on cyber security and crimes

(v) Encouraging, promoting and development of skills in cyber security crime scenario in public administration by the police for thorough investigations and prosecutions.

(vi) Establishing of legislation on cyber security among the public sectors and public administration institutions and organizations.

(vii) Establishment and protection of the National Cyber-security system ,awareness and developing expertise in cyber security

(ix) Enhancement and increase in the resilience of information systems of the public administration.

(x) Ensure effective protection and response to cyber- attacks incidents and strong international co-operation with other countries regarding cyber security.

KEY SECURITY TRENDS IN ORGANIZATIONS AND NATIONAL ECONOMY

According to Gartner &IEEE, (2015), Cyber-attacks are in various phases in organizations and national economy are as follows:

- ***Increase Volume of Big Data and the Issue of Governance and Security of Data***: Big data otherwise known as datasets are growing sporadically and shared worldwide in this 21st century .This data needs to be protected in public administration for the public

interest, hence ,this requires for new storage against cyber criminals such as cloud storage.

- ***Diversity of Mobile Devices (Bring Your Own Device)***: This model of BYOD poised a serious threats of cyber criminals in public administration as this is use to penetrate organizations (both private and public) using Trojan horse to affects the network and employee devices must be thoroughly examined and updated where necessary.
- ***Security and Privacy of Cloud***: This is now common to cloud services and there is much breach of security in this services as its takes longer days, weeks and several months before, it would be discovered and this would have caused great attacks.
- ***Need for Tracking the Movement of Data within the Organization:*** Series of criminal activities occurs in public sector organizations where data theft and attacks are gaining ground through malicious software, hence, cyber security technologies needed to be installed to monitor various users and employees within the organization.
- ***Attacks to Destroy:*** Hacktivist group averred that, series of attacks will be directed to company and public organizations for their own interest in terms of discovering vulnerable areas in the organization's database or technologies.
- ***Safety Risks Associated with Computerization of Public Administration (e-government)***: procurement and installation of new technologies sometimes poised a new threats and risks that threatened the safety of data in public administration and general public networks

FREQUENTLY USED ATTACK TECHNIQUES ON ORGANIZATIONS

According to Mcfe, (2015), the following are the frequently used attack techniques on organizations:

(1) **Distributed Denial of Service:** This is when the attackers make the resources unavailable for the legitimate users though bonnets and malware in the network with many zombies machines that is controlled by the attackers. This affects the retail trade, financial services ,telecommunication companies ,travel industry and information technology sector.

(2) ***Phishing***: This is an efforts to obtain important information such as username passwords ,credit card details ,pin code, account number ,unique id through trickish acts from a trust worthy entity .This usually done by the attackers using email ,short message service and telecommunication devices .

(3) ***Social Engineering:*** This method involves obtaining critical and important information of authentication and identification via social interactions with the targeted victims or persons through psychological tricks on a top and strategic employee in a bid to gain access to vital information on organization system .Hence, this method avoid the use of physical breaking into the system of the organization but manipulating employees in obtaining vital information from them.

(4) Data Breach and Information Loss :This is when unauthorized user gets access to organization system and purposively lost or delete huge amount of organization data. This thus involve breach of data through negligence ,malicious attacker or system glitch by attackers through manipulation of data causing serious harm to organization reputation ,trust and revenue.

(5) ***Malware:*** This is the installation of malware on a system and communicating vital information to the originator in background without the knowledge of system administrator hence, this is a serious and powerful tool to harm the organizations.

(6) ***Inside Attack:*** This is an internal threats by employee in the organization sharing sensitive information to outsiders to have access to organizations finance, data and other confidential and sensitive data.

(7) ***Social Site:*** This is when competing organizations post negative information and propagandas against an organization with the aim of reducing reputation and brand digital and social media.

NEGATIVE EFFECTS OF CYBER CRIME AND ATTACKS ON ORGANIZATIONS

According to PWC, (2012) the following are the suggested as the negative effects of cyber attacks on organizations:

- ***Economic Loss***: Cyber- crime is a serious effects on organizations and this results into a big loss to the economy of the organization.
- ***Reputational Loss***: Any cyber- attacks results to organization loss of trust and belief by its loyal customers as this drives them away from being patronizing the company's products and services.
- ***Loss of Intellectual Property:*** Cyber- attacks and threats make organizations lost its patent and copy right ,trade secret through theft and this causes a huge loss to the intellectual properties of an organizations .
- ***Loss of Sensitive Business Information*** :Important value and worthy data of organization in terms of money are lost and this seriously harm the organizations in terms of opportunities of trade secrets worth of money to the advantage of the competitors.
- ***Lack of Trust***: Cyber- attacks to organization make customers to lost trust and not feel safe with the organizations as this shift their loyalty and patronage to other competitors .
- ***Disruption of Business Operations*** :Cyber-attacks to organizations results to lost of sales and disruptions of business operations for some period of time which if organization is not careful ,it might lead to automatic downfall of business organization.
- ***It Leads to Organization Equipment Loss:*** It is of the fact that, malwares destroys the entire network equipment of organization and this leads to serious expenses on the organization in re-installing the disrupted equipment.
- ***Reduction of Stock Price:*** The effect of cyber- attacks on organizations causes harm, thus, reduce the value and image of the organization with the use of malwares.

SECURITY THREATS, ATTACKS AND VULNERABILITIES

According to Kozik & Choras, (2013), threats ,attacks and vulnerabilities poised a serious issues to cyber –security as explained below:

- ***Vulnerabilities***: are weakness in a system or its design that permitted cyber criminals to implements commands or access unauthorized data and information and ensure denial of service attacks are found in hardware and software as well as weakness in policies.

- ***Exposure***: is an error in the system design and configuration which permitted cyber criminals to gather information ,hence , internet of things devices and applications should not be placed and located in a visible and easily accessed to by the criminals .
- ***Threats***: is an action that takes advantage of security breaches and weakness in a system, hence affect, the system negatively .The two basic threats under this are human and nature (earthquakes, hurricanes, floods, and fire).
- ***Attacks***: are actions engages in to harm or disrupt the normal function and operation by looking for vulnerabilities to exploits using tools and techniques by hackers and criminals. It is evident that , common cyber -attacks to public administration could be physical attacks ,denial of service attack, access attacks, attacks on privacy (eavesdropping ,tracking ,password attacks ,cyber espionage and data mining) ,cyber -crimes ,destructive attacks ,supervisory control and acquisition attacks.

METHODOLOGY

The research design adopted for this study is a descriptive survey design using secondary data as a means of data collection.

CONCLUSION

This study re-emphasized the importance and relevance of cyber–security strategy and awareness in combating cyber -crimes and attacks in Nigeria organizations and national economy as urgent attentions and proactiveness of governments is needed in Nigeria cyber space to prevent attacks and threats to the Nigeria environment.

RECOMMENDATIONS

(I) Governments should developed global and organized information exchange and implement cyber security standard as a policy in organization operational activities in line with 21st century cyber-security.

(II) Cyber security attack tools should be used to monitor the data flow activities in the organization.

(III) HR department and team should carefully carry out reference check on the background of employees before recruitment.

(IV) Organizations should implement cyber security standards like ISO 27001 to confirm their security.

(V) All software and hardware used by organizations should be standardized in line with set parameters.

(VI) Human Resources department in organizations should be trained regularly to create awareness about latest cyber attacking techniques.

REFERENCES

Abomhara, M. & Koien, G. (2014). Security and privacy in the internet of things. Current status Open issues in PRISMS 2014.The second international conference on privacy and-security in Mobile systems (PRIMS 2014).

Adhikari, E.(2017). ICT Framework, Retrieved from ICT Framework Network @https:/ict-frame.com /cyber-security-challenges-in-developing-countries/

Anczewski, L., Caelli, W. (2015). Cyber conflicts and small State.

Australia Bureau of Statistic, (2022).Australian Bureau of Statistics, https://www.abs.gov.au

Benazzouz ,C, Munilla, O., Gunalp, M, Gallissot & Gurgen, (2014). Sharing user I.O.T devices in the cloud ,Internet of things ,(WF-I.O.T).IEEE, World Forum.

Centre for Cyber-security Belgium 2.0,2021-2025 Tech.rep ,https:/kcb.be/sites /default/files /ccb_strategies%2020_Uk_WEB,pdf.

Challibinisk, K., Karpiuk, Kostrabue, (2021). The legal status of public enterprises and entities within the national cyber-security system ,Cyber security and Law

Czuryk, M. (2019). Supporting the development of telecommunications services and network through local and regional government bodies and cyber-security and law, 2019.

Documents /un/2018-survey/E-Government %20survey%2018_FINAL -%20 for %20-web.pdf.Accessed 15 October, 2019.

E-Government Survey, (2018).Department of Economic and social Affairs .United Nations, ,https ://public administration .un.org/egoukb/portals/egovkb/

Federal public service for foreign Affairs, Foreign trade & Development, (2022).Belgium at a glance https://www.belgium.be /sites/default/files /Belgium_at_a_glance_en-_pdf

Hooghe, L. & Mark, G. (2002). Types of Multi-level Governance .Les Cahiers Europeans de -sciences ,Po,doi :10.4337197814980904.00007.

International Telecommunication Union, (2018). Global Cyber–security index 2020.172.

Kaklausskaite ,M.(2020).Multi-level Governance in cyber-security ;What Roles for the European Regions ,European security Journal ,6.44-51,https ://cyber secforum.eu/wpcontent/uploads/2020/08/ECJ-VOLUME -6-2020-ISSUE-1pdf.

Karpiuk ,M.(2020).The obligations of public entities within the national cyber-security system ,Cyber-security and Law.

Kostrubiec, J. (2021).The Role of Public Order Regulations as Acts of Local Law in the performance of Tasks in the field of public security by Local self –Government in Poland, Lex Localis –Journal of Local self –Government ,2021,No. 19.

Kpzik, R., & Choras, M. (2013).Current Cyber security threats and challenges in critical infrastructures protection, in informatics and applications,(ICJA,2013)Second IEEE international conference,pp.93-97.

Nayak, S.D. (2013) impact of Cyber-Crime: Issues and Challenges.

Olumide, O.O, Victor, F.B. (2010): E-crime in Nigeria: Trends, Tricks and Treatment. The Pacific journal of Science and Technology, volume 11, Number 1, May 2010 (Spring)

Pramanik, S. (2013.Threat Motivation in Emerging Technologies for a smarter World (CEWIT,2013),10th international conference and Expo ,IEEE,PP1-5.

Schaeffer, B.S., et al. (2009): Cyber Crime and Cyber Security: A white Paper for franchisors, Licensors and others

Strassmann, P.A. (2009): Cyber Security for the Department of Defense, Retrieved July 10th, 2011 from https://www.strassmann.com/pubs/dod/cybersecurity-draft-vl.pdf

Thomas, M, Meyer ,S., Sperner ,s., Meissor & Brian ,T.(2012).On I.O.T –services, Survey, classification and enterprise integration in Green computing and communication (Green.com).

WEF (2019). The global risks report, world Economic Forum, Geneva, https ://www.weforum.