International Journal of Basic Science and Technology ISSN 2488-8648
December, Volume 6, Number 3, Pages 152 - 157 http://www.ijbst.fuotuoke.edu.ng/ 152

Cybersecurity - A Tool to Safeguard Digital Economy in a Developing Nation

[1]Etuk, E. A., [2]Etim,E.O. and [1]Ugwoke, F.N.
[1]Department of Computer Science, Michael Okpara University of Agriculture, Umudike, Nigeria
[2]Department of Computer Science, Abia State Polytechnic, Aba, Nigeria

Article Information

Article # 01019
Received: 24th Sept..2020
1st revision: 18th Sept. 2020.
2nd revision: 12th, Oct. 2020.
Acceptance: 24th Dec. 2020
Available on line:31st Dec. 2020

Key Words
Cybersecurity, Safeguard, Digital Economy, Developing Nation

Abstract

This piece of work was motivated by the exploding increase in the growth of digital technology in developing countries coupled with the inherent benefits of doing business on the internet and the need for the government to key in through the provision and implementation of necessary cybersecurity policy and strategy to curb the attendance risk therein. As a result, the purpose of this article is to raise knowledge, create trust, and confidence in the digital economy that modern technology advancements have fashioned into cyberspace. Several mitigation strategies were discussed ,with the goal of slowing the gains of the digital economy that have been caused by the acceleration of innovations and enterprise in digital space, as well as the amplification of vulnerability opportunities that malicious parties are waiting to take advantage of. Integrating national cybersecurity policy and strategy with the internet economy in developing nations will promote and enhance good governance, competitive cooperate organizations, ease of doing business, chatting a better path for a progressive nation, and most importantly trust among stakeholders in a secured digital economy.

*Corresponding Author: Etuk, E. A.: forgerals@yahoo.com

Introduction

One of the driving forces towards the ease of doing business in developing countries is the application of Information and Communication Technology (ICT). Because of the exponential expansion in internet access, millions of people in underdeveloped nations have seen a substantial and positive change in the way they conduct their economic operations: hence the digital economy. It can be assumed that soon most economic activities will be done digitally leading to economic growth and sustainability. Nigeria like most developing countries has keyed into this digital economic transformation which must be safeguarded through adequate cybersecurity programs.

In the opinion of the World Bank (2021) Newsletter, Africa should think big on digital development. At the current, incremental pace of economic and social advancement, too many of Africa's expanding youth population will be denied the opportunity to live up to their potential. Digital technologies offer a chance to disrupt this trajectory – unlocking new pathways for rapid economic growth, innovation, job creation, and access to services that would have been unimaginable only a decade ago. Yet there is also a growing 'digital divide', and increased cyber risks, which need urgent and coordinated action to mitigate. World Bank further maintains that Governments need to find more nimble and effective means of delivering services and interacting with citizens. Businesses need to utilize digitally-centered business models to connect with the hundreds of millions of customers previously out of reach due to geography or low income.

These digitally-centered business model identified by World Bank generates enormous data on daily basis. The ability to provide adequate privacy, data protection, and security to these data becomes an important issue due to the type of persons who access the internet, the volume of data generated, and limitations to unauthorized information. According to Punch (2021) The Executive Vice Chairman, Nigerian Communications Commission (NCC), Danbatta (2021), posited that trust and confidentiality will promote a healthy digital environment, as enshrined in global best practices to guarantee the privacy and integrity of digital data. The digital economy should be built on trusted technologies and partnerships, to ensure strong cybersecurity that rides on public confidence, security, privacy, and safety, to bolster responsive regulations, transparency, accountability, and digital governance. However, Danbatta acknowledges the pace at which technology advanced, acceleration of innovations and enterprise in the digital space amplified vulnerability opportunities, which malicious parties were quick to exploit, thereby slowing down the gains of the digital economy and

ISSN 2488-8648

that strong cybersecurity would reduce the surface of vulnerabilities in the digital economy that could be exploited.

Creating awareness, and disciplines used to provide privacy, data protection, and security cannot be overemphasized These include the technologies, devices, and products available to protect information systems and fend off the cybercriminals. There are numerous challenges confronting the digital economy in Nigeria ranging from unstable and poor supply of electricity to power computers and their peripherals, smartphones, network equipment, etc. Inadequate knowledge of cyberspace and cybersecurity by most citizens and the high cost of data services to Internet access is another challenge confronting the digital economy in Nigeria. This article will explore the knowledge and comprehension of the digital economy, as well as the significant job faced by cybersecurity stakeholders in raising awareness about the safeguarding and mitigation of numerous risks caused by excessive internet traffic.

Teoh and Mahmood (2017) noted that for the digital economy to thrive, the digital confidence of the stakeholders is high. Nations with high digital confidence like Singapore, depend less on the national level National Cyber Security Strategy (NCSS) to strengthen the trust and confidence in digital space. The NCSS is still a need as a foundation for the long-term strategy to cement the cybersecurity of the nation, as cyber threats and risks keep evolving. Singapore is beginning to intensify its efforts and commitment to national cybersecurity. The existing top ten nations in the digital economy have NCSS. It provides the necessary foundation for the digital economy to flourish further. An NCSS is not a requirement for a nation to begin a digital economy, however, NCSS is a requirement for a nation to continuously develop and be successful in the digital economy.

This article will explore the knowledge and comprehension of the digital economy, as well as the significant job faced by cybersecurity stakeholders in raising awareness about the safeguarding and mitigation of numerous risks caused by excessive internet traffic.

The Concept of Cybersecurity

International Telecommunication Union (2021) stated that cybersecurity 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 user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability, Integrity, which may include authenticity and non-repudiation, and Confidentiality. They are of the view that in cybersecurity various apparatus, rules and regulations, protective measures, and adequate management tactics in accompaniment with certain technologies must be established and adhered to.

According to Craigen *et al* .(2014), Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights." Articulating a concise, inclusive, meaningful, and unifying definition will enable an enhanced and enriched focus on interdisciplinary cybersecurity dialectics and thereby will influence the approaches of academia, industry, and government and non-governmental organizations to cybersecurity challenges.

Cisco (2020) defined Cybersecurity as the practice of protecting systems, networks, and programs from digital attacks. These cyber-attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative. Cybersecurity also known as information technology security or electronic information security and applicable in diverse contexts including business, mobile computing implies that computers, mobile devices, networks, servers, electronic devices, and most important data must be protected from malicious attacks. This concept can further be characterized into network security, application security, information security, operational security, disaster and business continuity, and End-user education. Here, they exposed cybersecurity in a multi-layered approach involving people who must understand and adhere to fundamental data security principles, processes adopted to speedily respond to attempted and successful security bridges, and technologies that empower with necessary tools needed to guard against the malicious occurrence.

Cavelty (2012) said Cyber-security is both about the insecurity created by and through this new place/space and about the practices or processes to make it (more) secure. It refers to a set of activities and measures, both

ISSN 2488-8648

technical and non-technical, intended to protect the bioelectrical environment and the data it contains and transports from all possible threats. This author's definition captures and pointed out where and how cybersecurity can take place and the methods therein for safeguards.

Types of Cybersecurity Threats Malware

Anti Virus Guard (2021) said that malware is any type of software created to harm or exploit another piece of software or hardware. Malware is a collective term used to describe viruses, ransomware, spyware, Trojans, and any other type of code or software that is built with malicious intent. It is this malicious intent that characterizes the malware definition — the meaning of malware is the damage it can inflict on a computer, computer system, server, or network. Therefore, it is the how and the why that separate one type of malware from the next. All viruses are malware, but not all types of malware are viruses. Viruses are just one type of malicious software.

Ransomware

Malwarebytes (2021) described ransom malware or ransomware as a type of malware that prevents users from accessing their system or personal files and demands a ransom payment to order to regain access. While some people might think "a virus locked my computer," ransomware would typically be classified as a different form of malware than a virus. The earliest variants of ransomware were developed in the late 1980s, and payment was to be sent via snail mail. Today, ransomware authors order that payment be sent via cryptocurrency or credit card, and attackers target individuals, businesses, and organizations of all kinds. Some ransomware authors sell the service to other cybercriminals, which is known as Ransomware-as-a-Service or RaaS.

Phishing

According to Pande (2017), phishing is a process of acquiring the personal and sensitive information of an individual via email by disguising as a trustworthy entity in an electronic communication. The purpose of phishing is identity theft and personal information like username, password, credit card number etc. may be used to steal money from user accounts. If a telephone is used as a medium for identity theft, it is known as Vishing (voice phishing). Another form of phishing is Smishing, in which SMS is used to lure customers.

Social Engineering

Cisco (2020) posits thus; social engineering is a completely non-technical means for a criminal to gather information on a target. Social engineering is an attack that attempts to manipulate individuals into performing actions or divulging confidential information. Social engineering threat types include: *Pretexting* - This is when an attacker calls an individual and lies to them in an attempt to gain access to privileged data. An example involves an attacker who pretends to need personal or financial data to confirm the identity of the recipient. *Something for Something (Quid pro quo)* - This is when an attacker requests personal information from a party in exchange for something, like a gift. Social engineering threats rely on tactics such as authority, intimidation, consensus/social proof, scarcity, urgency, familiarity/liking, and trust.

Denial-of-service

According to Cybersecurity and Infrastructure Agency (2019), a denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network. A denial-of-service condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. DoS attacks can cost an organization both time and money while their resources and services are inaccessible. Denial-of-service attacks don't just affect websites—individual home users can be victims too. Denial-of-service attacks can be difficult to distinguish from common network activity, but there are some indications that an attack is in progress.

NCC And Recent Cybersecurity Threat Alerts In Nigeria

There have been recent incursions into the Nigerian cyberspace, Punch Newspaper of November 15, 2021, reported thus: The Nigerian Communication Commission has said an Iranian hacking group known as Lyceum have been reported to start targeting telecoms, Internet Service Providers, and Ministries of Foreign Affairs in Nigeria and other African countries. The NCC said the group also known as Hexane, Siamesekitten, or Spirlin is targeting these companies with upgraded malware in recent politically motivated attacks oriented in cyberespionage. Information about this cyber-attack is contained in the latest advisory issued by the Nigerian Computer Emergency Response Team. The ngCERT rated the probability and damage level of the new malware as high.

According to the advisory, the hacking group is known to be focused on infiltrating the networks of telecoms companies and ISPs. Between July and October 2021,

ISSN 2488-8648
http://www.ijbst.fuotuoke.edu.ng/

Lyceum was implicated in attacks against ISPs and telecoms organizations in Israel, Morocco, Tunisia, and Saudi Arabia.

In the publication of Daily Post Newspaper, November 9, 2021, John Owen Nwachukwu reported thatThe Nigerian Communications Commission (NCC) has warned telecom consumers and the general public of a new Android malware that has been discovered. The malware, named '**AbstractEmu**', can gain access to smartphones, take complete control of infected smartphones and silently modify device settings while simultaneously taking steps to evade detection.

For the reasons adduced above on cybersecurity, The Australian Cyber Security Center (ACSC) according to Oladimeji *et al.* (2019) recommends that multi-factor authentication be implemented for users using remote access solutions, users performing privileged actions and users accessing important (sensitive or high availability) data repositories.

Digital Economy In Developing Nation

The term digital economy has several definitions from institutions, organizations, and individuals such as the World Bank, European Commission, Nigerian Communications Commission, Asia Development Bank, etc. All these meanings involve businesses that sell goods and services through the internet and digital platforms that facilitate and provide accessibility through spare capacity and demand. We will look at some of these definitions to bring more understanding. Digital economy refers to a broad range of economic activities that use digitized information and knowledge as key factors of production. The internet, cloud computing, big data, fintech, and other new digital technologies are used to collect, store, analyze, and share information digitally and transform social interactions. The digitization of the economy creates benefits and efficiencies as digital technologies drive innovation and fuel job opportunities and economic growth. The digital economy also permeates all aspects of society, influencing the way people interact and bringing about broad sociological changes (ADBI, 2018). Here the understanding of the digital economy emphasizes the impact created and the various benefits achievable where potentials of digital technologies are employed.

Toppr (2021) defined the digital economy as an economy that focuses on digital technologies, i.e., it is based on digital and computing technologies. It essentially covers all business, economic, social, cultural etc. activities that are supported by the web and other digital communication technologies. The term was first coined in the book "The Digital Economy: Promise and Peril in the Age of Networked Intelligence" by author Don Tapscott in 1995. There are three main components of this economy, namely; e-business, e-business infrastructure, and e-commerce. In the last 15 years, we have seen the tremendous growth of digital platforms and their influence on our lives. Now consumers are influenced by things they see on social media (Facebook, Twitter, Instagram) and other such popular websites. So, this economy is a way to exploit this opportunity. Now it is integrated into every aspect of the user's life – healthcare, education, banking, entertainment etc.

According to Mundulaand Auci(2019), the digital economy is a hyperconnected economy characterized by a growing interconnected people, organizations, and machines through the web and by the use mean of digital technology which includes: advanced manufacturing, robotics, and factory automation, new sources of data from mobile and ubiquitous Internet connectivity, cloud computing, big data analytics, and artificial intelligence. In their view, the digital economy brings people and organizations involved in business using superior technologies.

Cybersecurity and Digital Economy In Nigeria

A report from the Federal Ministry of Communication and Digital Economy quoted President MuhamaduBuhari on his mandate to the Federal Ministry of Communications and Digital Economy; The National Digital Economy Policy and Strategy (NDEPS) has been developed in line with the Presidential directives that were given to the Honourable Minister of Communications and Digital Economy on the assumption of office. Digital technologies are transforming every aspect of our lives and the NDEPS will enable Nigeria to take advantage of them to become a leading player in the global digital economy. Our desire to fast-track the development of our digital economy informed the decision to rename the Ministry of Communications to the Federal Ministry of Communications and Digital Economy. This expanded the Ministry's schedule to include the Digital Economy mandate and the development of our digital economy will facilitate the diversification of the economy. We are committed to the diversification of the economy and digital technologies will provide an important catalyst for this.

President Buhari in his speech at the launch of National Digital Economy Policy and Strategy (2020-2030)emphasized that "Globally, the Digital Economy is expanding at a very fast pace. In just a few years, this platform has transitioned from being a luxury to an absolute necessity. It is in recognition of this fact that we decided to re-designate the Federal Ministry of Communications as the Federal Ministry of

Communications and Digital Economy with a mandate to develop and implement a harmonized and well-coordinated digital economy policy and strategy for Nigeria".

Cybersecurity forms a vital hub for any digital economy. This essential infrastructure has the potential to stimulates the development of other sectors such as commerce, industry, agriculture, education, health, banking, defense, transportation, and social interaction and that is why Cavelty (2012), writes: "Cyber-security is both about the insecurity created by and through this new place/space and about the practices or processes to make it (more) secure. It refers to a set of activities and measures, both technical and non-technical, intended to protect the bioelectrical environment and the data it contains and transports from all possible threats".

The Federal Government has renewed its plans to safeguard Nigeria's digital economy from cybercrimes while building more trust among strategic stakeholders in the country and the Commission was interested in issues that would enhance, protect and boost Nigeria's digital economy. Trust and confidentiality will promote a healthy digital environment, as enshrined in global best practices to guarantee the privacy and integrity of digital data. The digital economy should be built on trusted technologies and partnerships, to ensure strong cybersecurity that rides on public confidence, security, privacy, and safety, to bolster responsive regulations, transparency, accountability, and digital governance.

Recommendations

From the foregoing, this piece of work recommend as follows:

1. That the federal government of Nigeria institutes without delay necessary guidelines that will strengthen the development of cyber security policies and strategies in the country.
2. That the skill gap on cybersecurity is closed through the introduction of cybersecurity courses in all tertiary institutions.
3. That government and organizations make effort in training and re-training her staff vertically and horizontally with the single aim of making the workers be abreast in the evolving cybersecurity techniques.
4. That institution involved in securing the nation's cyberspace be strengthened for a better national and international response to cyber-attacks.
5. That all the sub-sectors involved in the digital economy should be harmonized for proper coordination and integration into the cybersecurity policies. This will result in the creation of digitally centered businesses built on trust.
6. Governments need to find more nimble and effective means of creating awareness on cybersecurity issues for consumers and service providers.
7. Governments at all levels should encourage organizations to establish and develop incident response capabilities that will enable them to maintain detailed response plans of cyber-attacks.

Conclusion

Most developing countries are utilizing the expanding youth population, thriving mobile market, and growth in digital technology to tap the opportunities and great potentials offered by the digital economy. Unfortunately, there is also a growing digital divide advanced by increased cyber risks, which need crucial and coordinated action to mitigate. In this work, we have attempted to advance the course of cybersecurity as a tool to safeguard the digital economy in a developing country. The idea of the digital economy was also x-rayed to find ways through which the integration of cybersecurity tools can be used to promote trust and confidentiality. Safeguarding our cyberspace against theft, hacking, and damages of data, information, software, hardware, and disruption or misdirection of system services, fighting criminals, and keeping the necessary confidentiality, integrity, and availability of data and information through the development of good and sustainable cybersecurity will also guaranty a robust digital economy. This will enable the creation of more and new jobs, innovations, enhanced increase in productivity and efficiency in businesses, access to services, thereby accelerating general economic growth in developing countries.

References

ADBI. (2018). Understanding the Digital Economy: What Is It and How Can It Transform Asia? https://www.adb.org/news/events/understanding-digital-economy-what-it-and-how-can-it-transform-Asia

AVG. (2021). What Is Malware? The Ultimate Guide to Malware.https://www.avg.com/en/signal/what-is-malware#topic-1

Cavelty, M. D. (2012). Cyber Security.Contemporary Security Studies. Oxford University Press.

Cisco. (2020). Cisco ITC Cyberops Network Acad : ttps://www.cisco.com/c/en/us/products/security/html

Craigen, D., Nadia, D.T. and Randy, P. (2014). Defining Cybersecurity. publication/267631801 https://www.researchgate.net/.

Daily Post Newspaper (2012). New malware, AbstractEmu attacking, destroying Android phones – NCC warns Nigerians. https://dailypost.ng/2021/11/09/new-malware-abstractemu-

ITU. (2021). Introduction to Security Cyberspace, Cybercrime, and Cybersecurity.https://www.itu.int/en /ITU-D/Cybersecurity/

Mundula, L. and Auci, S. (2019). Institutional Entrepreneurship, Trust, and Regulatory Capture in the Digital Economy. IGI Global.https://www.igi-global.com/chapter/institutional-entrepreneurship-trust-and-regulatory-capture-in-the- digital-economy/215190

NCC. (2019). Federal Ministry of Communications and Digital Economy. President's Mandate. National Digital Economy Policy and Strategy (2020-2030). https://www.ncc.gov.ng/docman-main/industry-statistics/policies-reports/883-national-digital-economy-policy-and-strategy/file

Oladimeji, S. A., Agbakwuru, O. A., Opara, C. C. and Etim, E. O. (2019). Development of a Secured Database System for Higher Educational Institutions in Nigeria. International Journal of Advanced Research in Science, Engineering and Technology, 12(6) ISSN: 2350-0328.

Pande, J. (2017). Introduction to Cyber Security. Uttarakhand Open University, Haldwani ISBN: 978-93-84813-96-3

Punch Newspaper. (2021). Iranian hacking group targets telecoms, ISPs, foreign ministries in Nigeria, others—NCC. https://www.punchng.com

Sadiq, O. (2021). Flubot: Things to Know about the New Virus that Steals Banking Details from Android Devices; pp23

Teoh, C. S. and Mahmood, A. K. (2017). National cyber security strategies for digital economy. 5th International Conference on Research and Innovation in Information Systems (ICRIIS). OI:10.1109/ICRIIS.2017.8002519.

Toppr. (2021). Digital Economy. Emerging Trends Business. https://www.toppr.com/guides/business-environment/emerging-trends-in-usiness/digital-economy/

World Bank. (2021). The Digital Economy for Africa Initiative Digit Economy for Africa Initiativehttps://www.worldbank.org/en/programs/all-africa-digital-transformational (worldbank.org)