ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 9, Issue 7 , July 2022

The Need for Cybersecurity Awareness for Sustainable and Conducive Atmosphere in Nigeria

Oladimeji S.A., Madu F.U., Ezurike O., Nwachukwu C.A.N , Egbe T.P

Department of Computer Science, Federal Polytechnic Nekede, Owerri

ABSTRACT: The wide use of digital media is making attackers smarter by the day. It is not new to hear that despite the tremendous benefits of cyberspace, some criminally-minded individuals are taking undue advantage of cyberspace to perpetrate evils. The risk and severity of cyber-attacks have clearly grown over the past few years. Since 2018, we have witnessed the most horrific cases of cybercrimes related to massive data breaches, flaws in microchips, crypto jacking, spamming and many others. Governments are responsible for protecting national security and public welfare. As Nigeria is tapping into the potentials of digital revolution, Nigeria will have to attach high level of seriousness to the established laws that address cyber threats and hold perpetrators of cyber-attacks accountable,establish organizations and programs that help with Cybersecurity, and allocate money for cyber-public awareness, defence research, and education. The federal government should start expending more funds on evolving research on Cybersecurity, Blockchain technology, IoT, etc through FG-sponsored programmes. Any country that pays less heed to Cybersecurity will severely pay for the disasters that follow. This paper discussed cybersecurity awareness, cyber-attacks in Nigeria and provided counter-measures to mitigate cyber-attacks.

KEYWORDS: Cybersecurity, IoT, Blockchain, Cyberspace, & Cyber-attacks etc.

I.INTRODUCTION

The driving force behind cybersecurity is the threat of cyberattacks. Each level of a cyber-physical Infrastructure which consists of operational software, information, and people is susceptible to security breakdown, whether through attack, data breach, infiltration, or accident. Through Inter-connected computer, a belligerent cyber actor may conduct a cyber-attack with minimal technical and operational resources. With a minimal chance of failure, cyber-attacks offer a high return for a low financial investment. Because of the permeable nature of sophisticated networks, a cyber actor may infiltrate an adversary network with minimal risk of discovery [1] The increasing trend of ubiquitous computing with cyber threats is characterized by an attacker, a target system, a set of actions against the target, and the consequences resulting from the attack. Consequences include damages to the target, direct and indirect losses to victims, and variable impact on third parties. As cyberspace becomes increasingly pervasive and entrenched in society, it spawns the availability of more targets to attack, and an increase in the population of skilled attackers [1] Defenders must familiarize themselves with the environment by understanding not only the cyber domain but also the human element, the attacker, their motives and goals. Consideration of the identified key components will provide greater fidelity to the orientation phase of the decision-making process.

Cyberspace is a global domain within the information environment, consisting of the interdependent network of information technology (IT) infrastructures, including the Internet, telecommunication networks, computer systems, and embedded processors and controllers. Associetal dependency on information technology grows, so do cyber threats. A diverse group of nation-states, non-state actors, state-sponsored groups, and individuals may wage malicious cyber-attacks on a target [3] In support of the national security strategy, the nation must institute a multilateral strategic framework that focuses on the dynamic challenges of cyber in the Information Age.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 9, Issue 7 , July 2022

II. CYBERSPACE

Physical space is the dimension most often associated with security. Physical space whetherland, sea, or atmosphere, is demarcated into territories under the jurisdiction of sovereign statelaw. Throughout history, armies have been deployed across territories and bodies of water whether they were provinces, kingdoms, countries, or whole empires-in order to defend theirown land or lay claim to other lands (in the name of security or national aggrandizement) Conversely; cyberspace is unconfined to a spatial dimension or effectively sanctioned by sovereign states or international law. Globally interconnected, cyberspace is a realm of digital information and communication that consists of decentralized computer networks with no single authority to supervise or regulate operation [6] In the past several years, cybersecurity has transitioned from an esoteric concept only comprehended by computer scientists and information system managers to a national security threat requiring the attention of the public and policy makers. President Barack Obama has one time declared America's digital infrastructure to be a "strategic national asset" [6].Because of this idiosyncrasy, *The National Strategy to Secure Cyberspace* has emphasized that securing cyberspace is a global matter due to the interconnectedness of the world's computer systems. Conventional based policies, strategies, and initiatives from years past do- not directly address the new challenges and issues independently unique to the cyberspace domain, nor do they completely coincide with the legislation and agenda of foreign nation-states. Securing national cyberspace will require national cooperation to raise awareness, share information, promote security standards, and investigate and prosecute cybercrime (Aniekan, 2017).

III. THE CYBER ATTACKER (THE HUMAN ELEMENT)

Technology is normally associated with cybersecurity; however the human element cannot be disregarded. United States Air Force colonel John Boyd argued that "Machines don't fight wars, Humans fight wars." A cyber threat is always given its existence from ahuman element. A wide spectrum of malicious cyber attackers exists from individual hackers, to criminal enterprises, to terrorist groups, to corporations, to nation-states. [8] Fundamentally, each attacker can be classified into two, a sovereign state or non-state actor. A non-state actorwhose purposes are criminal and who is subject to the jurisdiction of one or more sovereign states includes hackers, criminal enterprises, terrorist groups, and corporations. Terrorists constitute a more serious set of non-state actors and are of concern both to law enforce mentagencies and national security agencies. According to some analysts, as many as twenty countries have cyber-war fare capabilities, including China, Russia and North Korea.State actors normally target other sovereign states, although specific targets may be identical to those of non-state attackers [8]. Unfortunately, these actors are not mutually exclusive and could amalgamate and create acustomized threat. The attackers do not need to amass great arms; it can all be done covertly and cheaply, by hiring outside expertise.

IV. MOTIVES OF CYBER ATTACKERS

In general, an active or high-profile cyber attacker will have a motive and goal to attack a target. A motive for an attacker would be to conduct espionage, obtain monetary gains, and inflict malicious harm or further national or ideological interests. When a cyberattacked acts based upon a motive, at least one of the following goals are attempted [10] Knowing what motivates hackers is a key part of keeping them out of your business IT systems.

A.Financial Gain

The primary motivation of a hacker is money, and getting it can be done with a variety of methods. They could directly gain entry to a bank or investment account; steal a password to your financial sites and then transfer the assets over to one of their own; swindle an employee into completing a money transfer through a complicated spear phishing technique, or conduct a ransomware attack on your entire organization. The possibilities are endless, but most hackers are out to make a profit.

B.Recognition & Achievement

Some hackers are motivated by the sense of achievement that comes with cracking open a major system. Some may work in groups or independently, but, on some scale, they would like to be recognized. This also simplifies the fact that cyber

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 9, Issue 7 , July 2022

criminals are competitive by nature, and they love the challenge their actions bring. In fact, they often drive one another to complete more complicated hacks (Buchanan, 2016).

C. Insider Threats

Individuals who have access to critical information or systems can easily choose to misuse that access to the detriment of their organization. These threats can come from internal employees, vendors, a contractor or a partner and are viewed as some of the greatest cyber security threats to organizations. However, not all insider threats are intentional, according to an Insider Threat Report from Crowd Research Partners[8]Most(51%) are due to carelessness, negligence, or compromised credentials, but the potential impact is still present even in an unintentional scenario.

D. Political Motivation (Hacktivism)

Some cybercriminal groups use their hacking skills to go after large organizations. They are usually motivated by a cause of some sort, such as highlighting human rights or alerting a large corporation to their system vulnerabilities. Or, they may go up against groups whose ideologies do not align with their own [8] These groups can steal information and argue that they are practicing free speech, but more often than not, these groups will employ a DDoS (Distributed Denial of Service) attack to overload a website with too much traffic and cause it to crash.

E . State Actors

State-sponsored actors receive funding and assistance from a nation-state. They are specifically engaged in cybercrime to further their nation's own interests. Typically, they steal information,including intellectual property, personally identifying information, and money to fund or further espionage and exploitation causes. However, some state-sponsored actors do conduct damaging cyberattacks and claim that their cyber-espionage actions are legitimate activity on behalf of the state [10].

F. Corporate Espionage

This is a form of cyber-attack used to gain an advantage over a competing organization.It is conducted for commercial or financial purposes like:

- Acquiring property like processes or techniques, locations, customer data, pricing, sales, research, bids, or strategies.
- Theft of trade secrets, bribery, blackmail, or surveillance.

V. CYBERCRIMES AND CYBER LAWS IN NIGERIA

Nigerians have become cyber-creatures, spending a significant amount of time online. As the digital world expands, so does cybercrime in Nigeria. The necessity to combat these seemingly uncontrollable phenomena gave rise to Cyber Laws in Nigeria. Cyber law acts as a shield over cyberspace, preventing cybercrime from occurring. The government is committed to developing and enforcing regulations to combat illicit online activities. The "Cybercrimes (Prohibition and Prevention) Act, 2015" has a significant impact on cyber law in Nigeria [15]. This Act creates a comprehensive legal, regulatory, and institutional framework in Nigeria to prohibit, prevent, detect, prosecute, and punish cybercrime.The Act also encourages cybersecurity and protection of computer systems and networks, electronic communications, data and computer programs, intellectual property, and privacy rights, as well as the protection of important national information infrastructure [15]

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 9, Issue 7 , July 2022

A. Cybercrime

Cybercrime is a type of crime that takes place in cyberspace, or in the realm of computers and the Internet. Because our society is evolving towards an information society where communication occurs in cyberspace, cybercrime is now a global phenomenon. Cybercrime has the potential to significantly influence our lives, society, and economy.

B. Cyber Law

Any law that deals with the internet and similar technology is known as cyber law. Cyber Law is frequently referred to as "Law of the Internet" or "IT Law." It's a legal framework for dealing with issues relating to the Internet, computing, Cyberspace, and other associated matters.One of the newest aspects of the legal system is cyber law. This is due to the rapid advancement of internet technology [14]. People who use the internet have legal safeguards under cyber law. This applies to both business and common citizens. Anyone who uses the internet should be familiar with cyber laws [7]
Intellectual property, contract, jurisdiction, data protection laws, privacy, and freedom of expression are all covered by cyber law. It oversees the distribution of software, information, online security, and e-commerce via the internet. E-documents are given legal validity in the field of Cyber Law. It also establishes a framework for e-commerce and e-filling.To put it another way, Cyber law is a legal framework for dealing with cybercrime. Due to the increased use of E-commerce, it is critical that suitable regulatory practices are in place to ensure that no malpractices occur [14].Cybersecurity laws vary a lot from country to country and jurisdiction to jurisdiction. Penalties depend on the nature of offence, and will range from a fine to imprisonment. It is critical for citizens to understand their particular countries' cyber laws in order to ensure that they are fully informed about all cybersecurity issues:

- Identity theft and impersonation
- Child pornography and related offences
- Cyberstalking
- Cybersquatting
- Racist and xenophobic offences
- Attempt, conspiracy, aiding and abetting
- Importation and fabrication of e-tools
- Breach of Confidentiality and Privacy
- Manipulation of ATM/POS Terminals
- Phishing, spamming, spreading of computer virus
- Electronic cards related fraud
- Use of fraudulent device or attached e-mails and website. (Nigerian Cybersecurity Act 2015)

VI. CASES OF CYBERCRIME IN NIGERIA

Cybersecurity threats and attacks have become rampant due to technology changes, social economic factors and inadequate criminal justice. Social media has a challenge to reporting cyber incidents as many people do not check the authenticity of news posted on social media.
Cybersafe Foundation, a cyber-security awareness creator, has called for more awareness in tackling the growing menace of cybercrime in Nigeria. Speaking at a forum for cyber security experts, mostly from the financial sector, and IT journalists, in Lagos, Cybersafe urged more collaboration among various security entities in the country [4]. While it was earlier revealed at another forum that Nigeria had lost about N5.5 trillion to fraud and cybercrimes in 10 years, the experts at the Cybersafe forum, in their various presentations warned that cyber security threats and attacks are not going away, as the phenomenon could constitute the next pandemic, spelling out dangers to corporate bodies, government and individuals refusing to create barricades and walls for their platforms, digital tools and applications against cyber-attacks. Some of those, who spoke at the event include MrsFavour Femi-Oyewole, Group Chief Information Security Officer, Access Bank, AbumereIgboa, Chief Information Security Officer, Stanbic IBTC, Dr. Obadare Peter Adewale, Chief Visioner at Digital Encode, Confidence Staveley, Cybersafe Foundation and Bharat Soni, Chief Information and Security officer at GTB Limited [4]
Femi-Oyewole, while warning that cyber-attacks could be the next post-COVID pandemic, said it was important for organisations and individuals to begin to build resilience and back-ups for their systems, platforms and applications. [7]

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 9, Issue 7 , July 2022

She urged organizations to check their ability to bounce back, should they suffer any attack. “If anything happens to you, how quickly can you bounce back? Have you checked your resilience, do you have a backup?” she asked. Saying that integrity, confidentiality and availability of a good cybersecurity system matters. “You need to put necessary measures in place to quickly detect breaches and remedy. Vulnerability is any flaw or weakness that can be exploited.
“There is a need to put in counter-measures to prevent, minimize or report any breaches on time so that corrective measures can be taken immediately.” According to her, the most important and first level of shield and line of defense against cyber-attacks is the human beings who should ensure that they do not open their systems and media platforms vulnerable.From his perspective, Soni, who listed the most recent cyber security breaches to include Twitter compromise of2020, Colonial Ransomware attack 2021 and cyber breach of an undisclosed Nigerian Bank 2021, said organisations should work to mitigate cybersecurity challenges such as insider fraud, business email compromises, ransom ware and phishing[4]According to him, cybersecurity threats and attacks have become rampant due to technology changes, social economic factors and inadequate criminal justice, adding social media has a challenge to reporting cyber incidents as many people do not check the authenticity of news posted on social media. Although we are highly regulated, we still need to know how to protect ourselves, while we enjoined IT journalists to adequately equip themselves with knowledge of trends in the cybersecurity ecosystem so they could help inform the public more accurately and actively.

A.Corps member bags two months for cybercrime

Justice Inyang Ekwo of the Federal High Court, Abuja, recently sentenced a member of the National Youth Service Corps (NYSC), AjayiTemitopeAyokunle to two months imprisonment without option of fine. [4] The 30-year old corps member, who posed as Dr. Joshua to defraud an American citizen, Maria, of $1,000 will in addition to his imprisonment, forfeit a cash sum of $500 found in his bank account and a sophisticated android telephone to the Federal Government. Justice Ekwo, who expressed utter disgust at the embarrassing rate of cybercrime among Nigerian youths, turned down the plea bargain entered by the convict with the Economic and Financial Crimes Commission (EFCC), wherein, he confessed to committing the crime and requested for a soft landing.

B. **Lagos Prince, one other jailed in Ilorin for Cybercrime**

Justice SikiruOyinloye of the Kwara State High Court sitting in Ilorin has slammed a 6-month jail term on one OyekanAbdulbaqqiAdedoyin, a self-acclaimed prince from Kosofe Local Government Area of Lagos State, for offences bordering on cybercrime.Prince Oyekan, 25, was jailed alongside one Oni Stephen Oluwaferanmi from Ilesha, Osun State.The duo of Prince Oyekan and Oni were prosecuted on separate charges by the Ilorin Zonal Command of the Economic and Financial Crimes Commission (EFCC).[4] They pleaded guilty when the charges were read to them.Upon their pleas, counsel to the EFCC, Andrew Akoja, led witnesses to review the facts of the two cases. The witnesses who are operatives of the Commission narrated how the defendants were arrested based on credible intelligence.

VII. CYBERATTACK TRENDS

Cybercrime is the broad umbrella under which actions that are performed using cyberplatforms are considered criminal under justice systems. [12] This may include online child sexual exploitation, money laundering through cryptocurrencies, funding and promoting terrorist organizations, and using the dark web for selling drugs and related criminal services. For the purpose of this paper, “cybercrime” is defined as, “cyberactions performed by non-state actors that violate criminal law, and may or may not have a political or national security purpose”. Cyberattacks can be further categorized by state and origin as active or passive.An “active" attack aims to alter system resources or affect their operation. Conversely, a "passive" attack seeks to use information from a system but does not affect system resources. Instead, passive attacks aim to obtain data for an offline attack. The term “data breach” is used interchangeably with “cyberattack”. Figure 1 illustrates the relationship between cybercrime, cyberattack and cyberwarfare [12]

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 9, Issue 7 , July 2022

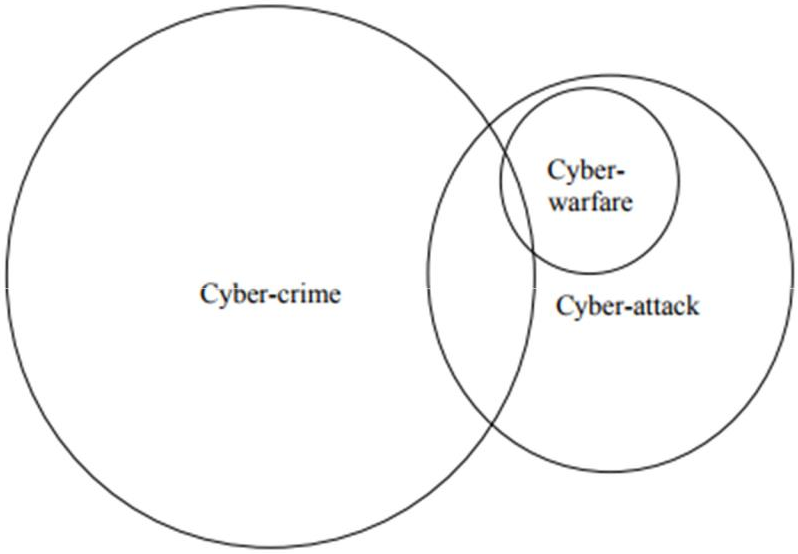

Figure No. 1: Relationship between Cyber-actions

Cyberattacks are on an upward trend. The Breach Level Index developed by a private company, Gemalto, shows that the number of data records compromised in data breaches by hacktivists, malicious insiders, malicious outsiders and state sponsors, and through accidental loss increased by 86 per cent since 2015, globally. Carbon Black, a cybersecurity company, reported that the dark web marketplace for ransomware has grown at a rate of over 2,500 per cent each year. Among web application attacks,Akamai reported that the United States is the largest target. In the Asia-Pacific region, Japan followed by Singapore and India have suffered the highest number of web application attacks during the second quarter of 2017, according to their live monitor of web-based attacks.Organizations in certain countries are more likely to experience data breaches. Based on a four-year study by IBM and the Ponemon Institute, South Africa and India have the highest estimated probability of data breach occurrences in the next 24 months, while Germany and Canada have the lowest. Arbor Networks analysed that enterprises, governments and educational institutes are most concerned with distributed denial-of-service (DDoS) attacks through social engineering and APTs on corporate networks [13]
According to IBM, the biggest threats in cybersecurity over the past few years have been from phishing attacks, DDoS attacks and malware (especially ransomware). However, CompTia's*2016 InternationalTrends in CyberSecurity*report states that 58 per cent of global firms struggle more with security threatscaused by human errors than technology risks, an issue that 61 per cent say has become more of a risk over the past two years.The motivations behind these attacks are diverse. Table 1 aims to summarize some of the cyber attack motivations and examples, while Figure 2 illustrates the trends by year and type of security incidents, developed by IBM. Figure 3 shows the number of cyberattacks in Asia-Pacific countries that have been verified by media report between 2013 and 2017, based on data from Gemalto's Breach Level Index, and Figure 4 shows the number of cyberthreats logged in the third quarter of 2017 in Asia-Pacific countries, based on data from Akamai's Real-Time Web Monitor.[13]

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 9, Issue 7 , July 2022

Table 1: Examples of Cyberattack motivation categorization

	Nuisance	Data Theft	Cybercrime	Hacktivism
Objective	Access and Propagation	Economic and political advantage	Financial gain	Defamation, press and policy
Example	Botnets and Spam	Advanced persistent threats	Credit card theft	Website defacement

Figure No. 2: Sampling of security incidents by attack type, time and impact (2015-2020)

VIII. NIGERIA'S CYBER VULNERABILITY TO CYBERCRIME

As government services go digital, criminals are spotting new opportunities for fraudulent claims and theft.

A. Digital revolution presents new risks: Around the world, the digitization of government is gathering pace, with a host of interactions now carried out online. In some countries, you can vote, pay bills and taxes, and get medical prescriptions – often using a single, digital citizen ID that's stored centrally. This has not escaped the attention of criminals that once focused primarily on retail banking and e-commerce. We are seeing a rise in fraudulent personal and corporate tax and VAT returns and associated rebates, along with bogus welfare claims [14]

B. Data leakage to Fraudsters: Data is leaking from both public and private sector organizations, either due to malicious hacking or rogue employees. Globally over 700 million personal data records were compromised in 2015, with the largest single breach exceeding information on 70 million individuals. Cyber criminals are also getting better at 'social engineering,' in the form of subtle emails or phone calls from apparently legitimate sources such as banks, financial advisers or even lawyers. In some cases these emails are even sent from the IT systems of those trusted advisers once the cyber-criminal has broken into their email system – the so called business email compromise fraud [14]

C. Cloud and BYOD: There is the need to continually monitor your cloud suppliers, carrying out audits to ensure ongoing compliance. In an increasing number of cases suppliers recognize this requirement and will offer a range of independently assured security certifications giving customers confidence in their ability. Governments may of course implement their own secure private cloud solutions, offering the ability to impose stricter standards and separation, albeit at increased cost and loss of economy of scale. The BYOD phenomenon impacts all organizations. Government and supplier employees are more frequently using their own smartphones, tablets and laptops for work [16] Management should ideally establish an organization-wide BYOD policy, as well as taking steps to bring mobile devices under management and ensure that sensitive data can only be accessed and processed by secure applications over secure encrypted channels. All employees should be familiar with the acceptable use rules for BYOD on corporate networks, and these rules should also make clear the rights of management to delete data from personal devices in the event of theft or the owner leaving the organization.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 9, Issue 7 , July 2022

D. IT outsourcing: Shared services, outsourcing and cloud are shifting provision outside of government, and one big challenge is to retain a core of in-house security expertise which ensures government remains an intelligent customer of such services, as well as having ready access to key skills. After all, people skilled in incident management, analytics, detection, monitoring and response services are scarce and in high demand. Many public sector agencies are living with financial constraints, and need to find creative ways to attract and develop cyber security professionals [14]On the other side, outsourcing could actually improve security, as cloud service providers tend to have relatively advanced cyber security, when compared to the legacy systems and outdated software which can be prevalent in many government IT infrastructures.

IX. MOST COMMON TYPES OF CYBER ATTACKS

Cyber-attacks can take many forms, and the sophisticated methods used by hackers and criminals are constantly evolving. A cyber-attack will usually take place in one of the following ways:

- **Denial-of-service (DoS) or distributed denial-of-service (DDoS) attack.** This type of attack floods network servers or systems, using bandwidth and rendering them unusable.
- **Malware.** This attack occurs when a system user clicks a link or opens an email attachment, which can then install software on the machine to block access (ransomware) or obtain information (spyware).
- **Phishing.** This occurs when a cyber attacker attempts to steal sensitive information, such as a credit card number or login information, by posing as a trustworthy source.
- **Man-in-the-middle (MitM) attack.** These take place when an attacker inserts themselves into a two-party transaction, such as obtaining information from a device connected to an unsecure public Wi-Fi network.

As technology has progressed in recent years, the opportunities for cyber criminals have increased. Large organizations - such as government agencies - are prone to lapses in security procedures which make them prime candidates for hackers.

X. WHAT NIGERIA MUST DO

As technologies mature and evolve, additional perspectives or new issues are expected to emerge. Governments can best ensure the protection of critical assets in cyberspace by ensuring the following principles for authentication policy:

A. Ensure the privacy of individuals: In the age of Big Data, the massive amounts of data generated and collected, sold and traded by third parties are a worrying trend globally. With AI, businesses can analyse more complex data and get more accurate results. Today, online services and smart devices are constantly collecting users' data, including sites visited, purchases made, geolocation, Wi-Fi network information, voice and image recordings, and other personal details, thus potentially reducing users' privacy and safety. Similarly, using tracking AI in business networks capable of monitoring emails, documents and photographs of employees and their activities in the network is a sensitive topic. Employees should be trained and informed about company practices collecting personal data and the use of such data. To track the extent to which countries are safeguarding their citizens' privacy rights, a global cyberprivacy index could be developed.

B. Establish an incident reporting mechanism: This includes monitoring and assessing the occurrences of cyberattacks and data breaches, including their nature, scope and impact, as well as details of the responses to incidents. One of the challenges government officials may encounter is obtaining an accurate picture of the cyberrisks without an incident reporting mechanism. When Australia and New Zealand established a government audit process, there were 44 and 16 voluntarily reported data breaches in the respective countries. With the new Privacy Amendment (Notifiable Data Breaches) Act 2017 in Australia, the numbers are expected to increase dramatically as organizations are required to declare any "eligible data breaches".

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 9, Issue 7 , July 2022

C. Strengthen laws and legislations, and increase penalties for cyberattackers and hackers: There is no international framework that binds countries in terms of offensive cyberoperations, but some countries have started initiating the establishment of national laws and legislations to define responsibilities, increase penalties for various cybercrimes, and ensure citizens' safety and security.

D. Plan and implement digital safety and digital literacy initiatives: These initiatives could be supported by developing and updating cybersecurity policies in the private sector and government organizations, organizing training and awareness campaigns, and creating methods for measuring employees' compliance to cybersecurity standards and policies. It would be important to develop digital safety anddigital literacy indicators to better gauge the current state of cybersecurity awareness among individuals and organizations worldwide.

E. Invest in cybersecurity research and initiatives:- One of the common challenges faced by governments in the region is securing sufficient funding and investments to address

cybersecurity. The increasing level of sophistication in cyberattacks would require government officials to upgrade their cybersecurity knowledge and skills on a regular basis. Regional cooperation and knowledge sharing would also be crucial for addressing the wide range of cyberthreats and risks.

F. Promote cybersecurity best practices for individuals and organizations:- Although not exhaustive, some of the cybersecurity best practices for individual users include the following:

- **Clear cache in browsers and devices**:– This involves clearing browsing history, and removing stored passwords and related information. Clearing a browser's cache makes it more difficult for attackers to access personal information such as email passwords and bank account information. It is also important to change passwords regularly.
- **Update software regularly**:– Several hacks have been carried out by exploiting software vulnerabilities. Attackers exploit this weakness by writing codes to target a specific vulnerability. Software and system updates generally involve patching vulnerabilities, and improving operation system's functionality and performance.
- **Enable at least two-factor authentication for account log in**:- To deter password-guessing attacks, two-factor authentication can be helpful. With two-factor authentication, attackers will have to either acquire the physical component of the log in, or gain access to the cookies or tokens placed on the device by the authentication mechanism. Various account services such as Facebook, Google and online banking services offer two-factor authentication, and it is highly encouraged.
- **Know your right to privacy**: – The Cookie Law is a privacy legislation in Europe that requires websites to obtain consent from visitors to store or retrieve any information on a computer,smartphone or tablet. Individuals have the right to refuse the use of cookies to track browsing history. In addition, review privacy policies and adjust privacy settings of the sites used, particularly, social media sites.
- **Do not automatically connect to Wi-Fi networks and store Wi-Fi passwords**: – As discussed above, public Wi-Fi networks are vulnerable to hacks and pose security risks

XI. CONCLUSION

The frequency of cyber-attacks is increasing, and government and private digital entities in Nigeria are the most vulnerable. Staying one step ahead of cyber criminals is not an easy task, but implementing robust, proactive security processes is the most effective way to deal with this dangerous threat. In creating a safe, digital environment for citizens and companies, government can embrace leading practices from the private sector, and encourage employees to be more cyber-aware. Nigeria will have to attach high level of seriousness to the established laws that address cyber threats and hold perpetrators of cyber attacks accountable, establish organizations and programs that help with Cybersecurity, and allocate money for cyber-public awareness, defence research, and education. The federal government should start expending more funds on evolving research on Cybersecurity, Blockchain technology, IoT, etc through FG-sponsored programmes. Any country that pays less heed to Cybersecurity will severely pay for the disasters that follow. This paper discussed cybersecurity awareness, cyber-attacks in Nigeria and provided counter-measures to mitigate cyber-attacks.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 9, Issue 7 , July 2022

REFERENCES

[1] Ajiji, Y. M. (2017). "Cybersecurity Issues in Nigeria and Challenges." International Journal of Advanced Research in Computer Science and Software Engineering 7(4): 315–321.
[2] Alagappa, M. (1987). The National Security of Developing States: Lessons from Thailand. Dover, MA: Auburn House.
[3] Alkali, R. A. (2010). Issues in Nigerian Foreign Policy and International Relations. Kaduna, Nigeria: Media Press.
[4] Ameh O.(2021, November, 24) 'Corps member bags two months for cybercrime. The Guardian,Nigeria.https://guardian.ng/news/corps-member-bags-two-months-for- cybercrime/
[5] Aniekan, M. N., &Afolabi, M. B. (2017). "Introduction to Cybersecurity and Cybercrime."In Aniekan&Afolabi (Eds.) Intelligence and Security Studies Programme. Lagos, Nigeria: Spectrum.
[6] Antonucci, D. (2017). The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities. Hoboken, NJ: John Wiley & Sons.
[7] Azeez, O. (2019). "Cybercrime Cost Nigeria N288 bn in 2018."Business a.m. https://www.businessamlive.com/cyber-crime-cost-nigeria-n288bn-in-2018/, accessed November, 25, 2021.
[8] Buchanan, B. (2016). The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations.New York: Oxford University Press.
[9] Buzan, B., & Hansen, L. (2009). The Evolution of International Security Studies. New York: Cambridge University Press.
[10] Cavelty, M. D., & Wenger, A. (2019). "Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science." Contemporary Security Policy 41(1): 1–28.
[11] Federal Government of Nigeria (2015). Nigerian Cybersecurity Act 2015. http://lawnigeria.com/LawsoftheFederation/Cyber-Crime-Act,-2015.html. Accessed January 25, 2022.
[12] Frank, I., & Odunayo, E. (2019). "Approach to Cybersecurity Issues in Nigeria: Challenges and Solutions." (IJCRSEE) International Journal of Cognitive Research in Science, Engineering and Education 1(1): 1–11.
[13] Global Cybersecurity Index (2019). 2019 Global Cybersecurity Index.https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx. Accessed December 20, 2021.
[14] Mohamed A.H,&Solanke, A. A. (2019). "Cybercrime and Digital Forensics: Bridging the Gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria." International Journal of Cybersecurity Intelligence and Cybercrime 2 (1): 56- 63.
[15] Mordi, M. (2019). "Is Nigeria Really the Headquarters of Cybercrime in the World?" Guardian. https://guardian.ng/news/is-nigeria-really-the-headquarters-of-cybercrime-inthe-world/. Accessed October,18, 2021.
[16] Wada F. and Odulaja G. O. (2014), "Electronic Banking and Cyber Crime In Nigeria - A Theoretical Policy Perspective on Causation," Afr J Comp & ICT, Vol 4(3), no. Issue 2.