# THE MENACE OF CYBERCRIMES: STUDYING THE STRATEGIES OF STRENGTHENING CYBER SECURITY AND RESILIENCE TO MITIGATE CYBERCRIMES IN NIGERIA AND THE GLOBE

BY

AKPAN, E. Ebenezer, *Ph.D, FCICN, AP, PPGDCA, PHDCDPM*
Corporate Institute of Research and Computer Science
140 Ikot Ekpene Road
Uyo, Akwa Ibom State

AND

David K. WILSON, *Ph.D*
Department of Library and Information Science
Faculty of Education
University of Rochester
Rochester, New York City

## ABSTRACT

*The study examined the extent of the menace of cybercrimes studying the strategies of strengthening cyber security and resilience to mitigate cybercrimes in Nigeria and the globe. Internet usage has been rapidly rising in Africa, as more people connect to the inter-web mostly through their mobile phones. This increased use has created a new challenge for the continent in potential attack vectors at both individual and organizational level. The increasing availability and utilization of internet facilities, threats in the cyber space have also escalated dramatically. Criminals are invading homes and offices not by breaking doors and windows but by breaking into laptops, Personal Computers and wireless devices through the internet. Cyber security has played a vital role in ensuring the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment - the internet. The study reviewed the origin of cybercrime, the cases of cyber attack in Nigeria, the cases of cybercrime globally and the strategies to strengthen cyber security and cyber resilience in Nigeria. On this basis, the study concluded that the alarming growth of the internet and its wide acceptance has led to increase in security threats. In Nigeria today, several internet assisted crimes known as cybercrimes are committed daily in various forms such as fraudulent electronic mails, pornography, identity theft, hacking, cyber harassment, spamming, Automated Teller Machine spoofing, piracy and phishing. It was therefore recommended that countries should build upon the work of the Global Community Engagement and Resilience Fund (GCERF) which supports local, community-level initiatives aimed at strengthening resilience against cyber-attacks.*

KEYWORDS: Cybercrimes, Strategies, Cyber Security, Resilience, Security and Resilience against Cyber Risk in Nigeria

## Introduction

It is obvious that technology adoption is driving business growth and innovation in Nigeria, at the same time it is exposing the country to new and emerging threats. Cyber-terrorists, spies, hackers and fraudster are increasingly motivated to target our ICT infrastructure due to the increasing value of information held within it and the perceived lower risk of detection and capture in conducting cybercrime as compared to more traditional crime. According to Global Commission on Internet Governance (2015), internet usage has been rapidly rising in Africa, as more people connect to the inter-web mostly through their mobile phones. This increased use has created a new challenge for the continent in potential attack vectors at both individual and organizational level. Juwah (2015) opine that with the increasing availability and utilisation of internet facilities, threats in the cyber space have also escalated dramatically. Criminals are invading homes and offices not by breaking doors and windows but by breaking into laptops, Personal Computers and wireless devices through the internet. The global economic loss due to cybercrimes and cost of systems repairs as a result of cyber attacks runs into billions of naira every year.

Debates on cybercrime and cyber security tend to concentrate around dramatic events such as the defacement of popular online spaces, sensitive information leaks or diffusion of particularly infectious malware (Schneier and Bruce, 2016). Less attention has been paid to broader issues of cyber resilience, that is, an organization or government's capability "to withstand negative impacts due to known, predictable, unknown, unpredictable, uncertain, and unexpected threats from activities in cyberspace" (ISACA, 2014). Cyber Resilience refers to the idea that failures will inevitably occur, but promotes the adoption of holistic, cooperative measures that ensure a system does not wholly collapse.

The EVC have noted that if users are to benefit from the full advantages of the internet, confidence in the information infrastructure is of utmost importance. "Cyber threats such as malware, cyber harassment, spoofing, phishing, spam, hacking, viruses, Trojans, worms, child online pornography and spyware are becoming extremely sophisticated. This is especially true with increased presence of organised online criminal groups. The internet has long ceased to be the exclusive domain of the technically savvy users. User friendly software and interfaces enable all types of users including novices and children to interact remotely. This new territory contains a goldmine of valuable information and potential victims. The complicated infrastructure of the internet, also makes it more difficult to track down criminals".

Juwah (2015) revealed that the commission receives complaints frequently from International Criminal Investigation Organisation (ICIO), Police and EFCC on cybercrimes committed by some Nigerians on the internet both locally and abroad. He opined that though, national measures are being taken by individual nations, cyber threats remain basically an international problem. "The internet is a borderless communication tool and consequently, any solution to secure it must involve global collaborations. Loopholes in legal framework are being exploited by perpetrators as harmonisation between existing laws across nations is far from satisfactory. Cross border investigation and prosecution are difficult if categorisation of crimes differ from country to country. This study therefore seeks to assess cyber security and resilience in Nigeria.

According to Kaplan, James and Tucker (2015), the global digital economy, democracy and the public sphere now completely depend upon the stability and security of cyberspace. Encryption technologies are necessary to protect data privacy, authenticate websites and secure online transactions. Security problems such as consumer data breaches and denial-of-service attacks disrupt the digital economy and the public sphere. They also can have chilling effects on speech and online behaviour. Perlroth and Nicole (2016) asserts that as everyday physical objects from cars to home appliances increasingly become internet-connected, human safety in the real world also depends upon cyber security. Trust in digital infrastructure is now necessary for the capacity to communicate, access knowledge, use one's banking system, drive a car and buy products through an online commerce site such as Amazon. Democracy also depends upon cyber security, considering the stunning admission by United States intelligence agencies about Russia's influence campaign, probing of voter rolls and hacking of Democratic National Committee emails during the 2016 presidential campaign.

Cyber security is one of the great human rights issues of our time. Cyber security is not only an issue for "Internet users" but for all citizens. Even someone who has never been online is directly affected when a retail company they frequent (for example, Target or Home Depot) experiences a massive consumer data breach, when their television potentially becomes a surveillance tool or when they are denied medical care because of a ransomware attack that cryptographically locks medical records and otherwise disables health care provider systems. All people and all societies are now directly affected by the security of digital systems (Schneier and Bruce, 2016).

## Concept of Cyber Crime

According to BlueVoyant (2023), Cybercrime is any criminal activity involving a computer as the target or tool of the crime. The U.S. Department of Justice (DOJ) groups cybercrime into three main categories:

***Hacker attacks***: Utilize computers as a weapon.

***Network penetration***: Target a computer or other devices, attempting to gain unauthorized access to a network.

***Computer-assisted crimes***: Computers are not the main tool or target but play an instrumental part. For example, using a computer to store files downloaded illegally.

## Origin of Cybercrime

Cybercrime first started with hackers trying to break into computer networks. Some did it just for the thrill of accessing high-level security networks, but others sought to gain sensitive, classified material (Schubert, 2022). Eventually, criminals started to infect computer systems with computer viruses, which led to breakdowns on personal and business computers. They following are list of cybercrime:

The first cybercrime began with good intentions and ended with unexpected consequences. In 1988, Cornell University graduate student, Robert Tappan Morris, developed a program to assess the size of the internet. The program would crawl the web, install itself on other computers, and then count how many copies it made. Once tallied, the results would indicate the number of computers connected to the internet. Unfortunately, problems arose for Morris, who struggled to ensure accuracy. Morris made a command that forced the worm to install itself on a computer every one out of seven times; even if the computer claimed it already had the program. With each installation, the infected computers would become further debilitated until they finally crashed (Climer, 2018). It was the first Distributed Denial of Service (DDoS) attack, and it was entirely by accident. In total, the worm damaged approximately 6,000 computers (10% of the entire internet at the time). The estimated cost of repairing the effects of the worm range between $100,000 and $1 million or between $201,000 and $2.9 million adjusted for inflation. Morris was charged with the violation of the Computer Fraud and Abuse Act, and his sentence included fines, plus three years of probation and community service.

## Cases of Cybercrimes in Nigeria

Over the years, the alarming growth of the internet and its wide acceptance has led to increase in security threats. In Nigeria today, several internet assisted crimes known as cybercrimes are committed daily in various forms such as fraudulent electronic mails, pornography, identity theft, hacking, cyber harassment, spamming, Automated Teller Machine spoofing, piracy and phishing, (Omodunbi et al., 2016), Cybercrime is a threat against various institutions and people who are connected to the internet either through their computers or mobile technologies. The impact of this kind of crime can be felt on the lives, economy and international reputation of a nation.

According to Adepetun (2020) Small and medium-scale enterprises (SMEs) in Nigeria face more cyber threats with attacks increasing by 89 per cent last year. Kaspersky, a Russian multinational cyber security and anti-virus provider, disclosed this, noting that when a small business owner is faced with the responsibilities of production, financial reports and marketing at the same time, cyber security worry is an unnecessary challenge. According to Kaspersky researchers, which assessed the dynamics of attacks on SMEs between January and April 2022 and the same period in 2021, they warned that these threats pose an increasing danger to entrepreneurs. In 2022, the number of Trojan-Password Stealing Ware (PSW) detections in Nigeria more than doubled when compared to the same period in 2021 – 2654 detections recorded in 2022 compared to 1076 in 2021.

Cybercrime is on the rise in Nigeria with both an increasing number of victims and perpetrators. LSE Fellow Uche Igwe (2021), discusses the economic cost to the country in the global context, and the reasons why the Nigerian government should focus on collaborative interventions. An example is Ramon Olorunwa, aka Ray Hushpuppi, a man who was not exactly what he wanted the world to believe. He disguised himself as a philanthropist and businessman who flaunted his wealth with unique flamboyance and penetrating audacity. He would regularly adorn himself with fancy watches, designer clothes and showcase expensive car collections typical of a superstar. He hung out in style with other personalities and travelled around the world in private jets and luxury yachts, displaying bundles of US dollar notes openly. He had a growing global audience of 2.5 million predominantly young social media followers. Hushpuppi's public drama continued until he was arrested during the COVID-19 lockdown in June 2020 on charges of conspiring to launder millions of US dollars to finance his boisterous lifestyle. According to Dubai Police, Abbas and 11 other people were arrested during raids in which authorities seized nearly US$14 million, 13 luxury cars worth $6.8 million, 47 smart phones and computer evidence containing more than 100,000 fraud files on nearly 2 million possible victims. He has been extradited to the United States where he is currently detained and facing trial for cyber fraud, hacking and scamming.

According to Soonest Nathaniel (2021), The Nigeria Police Force National Cybercrime Centre (NPF-NCCC) has successfully busted two suspects responsible for computer-related fraud, identity theft, crypto currency fraud, and obtaining money by false pretence. The duo are said to run a syndicate specializing in defrauding unsuspecting victims from foreign countries by assuming appealing identities of other persons and promising them romantic relationships, under the pretext of which they defraud their victims. In the extant case, a report on their activities was received from Incheon Metropolitan Police Agency in Korea through the Interpol National Central Bureau that in May, 2021, the suspects approached the victim, one Baek Seong-hee, a Korean national, via Kakaotalk, a mobile messaging application used majorly in South Korea, in the guise of being a member of the US Armed Forces stationed in Yemen.

## Cases of Cybercrimes in the Nigerian banks

The Risk-Based Cyber security Framework and Guidelines for Other Financial Institutions (OFIs) recently released by the Central Bank of Nigeria (CBN) could not have come at a better time given the growing cyber security threats in the country. But it would not work except the banks and other financial institutions show enough commitment to its implementation. The threats, identified by the CBN for the banks and financial institutions include ransom ware, targeted phishing attacks and Advanced Persistent Threats (APT) that have become prevalent within the system. The deadline for full compliance has been put at 1st January 2023.

Cybercrimes refer to those criminal acts such as identity theft and bank frauds facilitated through the use of the internet. To our collective shame, our country is often cited as a breeding ground for these nefarious practices because of the activities of some of our citizens. While cyber criminals in some other countries are using their negative skills for espionage and illicit technology theft, their Nigerian counterparts are using their skills to defraud individuals and companies. But it is not only abroad that these people perpetrate their criminal activities, they also do it at home. So endemic is the problem that the Senate recently disclosed that Nigeria has lost about $450 million to 3,500 cyber-attacks on its Information and Communications Technology (ICT) space, representing about 70 per cent of hacking attempts in the country. From social networking and research to business and commerce, ICT systems are ordinarily deployed to perform simple as well as complex tasks. But the cyberspace is also vulnerable to the activities of criminals. What marks out the Nigerian fraud gangs operating internationally is their focus on illicit financial and economic transactions. For instance, in June 2019, a damning statement by the American Department of Justice said, “Foreign citizens perpetrate many BEC scams. Those individuals are often members of transnational criminal organizations, which originated in Nigeria but have spread throughout the world.” Last year, no fewer than 12 Nigerians were charged in four criminal complaints in connection with their roles in expansive online fraud schemes (including romance scams and pandemic unemployment assistance fraud) targeting individuals in the United States. Some others were also charged with mail fraud, attempted mail fraud, and mail and wire fraud conspiracy, in connection with an advanced fee fraud scheme using social media to target elderly victims. In 2015, the Cybercrimes Act was passed into law to address the challenges. The law criminalizes a variety of offences – from ATM card skimming and identity theft to possession of child pornography. It imposes, for instance, seven-year imprisonment for offenders of all kinds and additional seven years for online crimes that result in physical harm, and life imprisonment for those that lead to death. But like almost every law in the country, there is the problem of enforcement. Committed mostly by the young, often called ‘Yahoo Boys’, a precursor of the infamous ‘419’ email scammers, the fraudsters are increasingly taking advantage of the rise in online transactions, electronic shopping, e-commerce and the electronic messaging systems to engage in all manner of crimes that have sullied the image of Nigeria abroad. To deal with such emblem of shame, there is an urgent need to improve the capacity of cyber security officials and the sharing of cyber security best practice from across the globe. In addition, we must build the capacity for local law enforcement. Given the importance of cyber security to the banking sector and indeed all financial institutions, we hope that they will heed the CBN directive by beginning to put in pace necessary compliance measures

According to Mihir Bagwe (2022), the alleged mastermind, 52-year-old Kehinde Oladimeji, was caught and arrested by the police, along with 27-year-old Olanrewaju Adeshina and 42-year-old Kolapo Stephen Abiodun, the police statement says. Another alleged syndicate member, Chibuzor Holland, who the police say came from France to execute this cybercrime, absconded.

The Sting Operation: The police made the arrests on March 30 as the result of a sting operation conducted by the police unit's commissioner, Anyasinti Nneka. The operation was based on intelligence received from "a leading New Generation Bank who is also a member of PSFU's Stakeholders' Forum," the statement says. At the time of the arrest, the gang members were recruiting an information and technology department employee at a bank "to perfect the hacking of the bank's network/posting application with [an] intent to pull-out huge sums of money," according to the statement. Abiodun, a former IT department employee at the same bank that the syndicate was planning to target, asked an unnamed current employee of the same bank's IT department to "leave critical gateways open on the Bank's server for the syndicate to gain unauthorized access into the network and move money out using Python application and Zoom," the statement says. In return, the employee was offered 200 million naira (approximately $473,500) and a visa to an undisclosed destination. During the sting operation, the PSFU also recovered several phones and other electronic devices from the accused. A forensic analysis of these devices showed that the syndicate had picked 10 banks "to be hacked using a similar method once the first attack [was] successful," the statement says. The gang also had personal and corporate bank account details, it says, "Which they ought not to have."

In a separate incident, the Nigerian police, as part of an internationally coordinated sting operation, have busted another cybercriminal gang, which Interpol calls "Killer Bee." The suspects are three middle-aged Nigerians, arrested for allegedly carrying out cyber fraud across Southeast Asia using Agent Tesla, a remote access Trojan, Interpol says. The operation was a coordinated effort between the Economic and Financial Crimes Commission of Nigeria, Interpol, the National Central Bureaus and law enforcement agencies of 11 countries across Southeast Asia, according to Interpol. The operation was initiated after Interpol's private sector partner Trend Micro provided operational intelligence to the agency about the "emergence and usage of Agent Tesla malware" in this case. Agent Tesla was found on the mobile phones and laptops of the syndicate members that were seized by the EFCC during the bust. "Through its global police network and constant monitoring of cyberspace, Interpol had the globally sourced intelligence needed to alert Nigeria to a serious security threat where millions could have been lost without swift police action," Interpol Director of Cybercrime Craig Jones says in the statement. "Further arrests and prosecutions are foreseen across the world as intelligence continues to come in and investigations unfold." The syndicate, operating from the west coast of Africa, targeted corporate, including oil and gas companies in Southeast Asia, the Middle East and North Africa, the statement says. Interpol adds that using Agent Tesla, the syndicate rerouted "financial transactions," which helped them steal confidential online details linked to these corporate. The three arrested individuals also had several fake documents, "including fraudulent invoices and forged official letters," Interpol says. The statement says that one of the scammers, Hendrix Omorume, has been convicted of three counts of serious financial fraud and faces 12 months in prison. The two other men are still on trial. "Cybercrime is spreading at a fast pace, with new trends constantly emerging. Through operations like Killer Bee, Interpol supports EFCC in keeping pace with new technologies and understanding the possibilities they create for criminals and how they can be used as tools for fighting cybercrime," says EFCC Director of Operations Abdulkarim Chukkol.

## Cases of Cybercrimes in Public Sector in Nigeria

Over the past decade, the internet has experienced an explosive growth with the number of hosts connected to the internet increasing daily at an exponential rate. As the internet grows to become more accessible and more services become reliant on it for their daily operation, so does the threat landscape. In Nigeria, cybercrime has become one of the main avenues for pilfering money and business espionage. According to Check Point, a global network cyber security vendor, as of 2016, Nigeria is ranked 16th highest country in cyber-attacks vulnerabilities in Africa (Ewepu, 2016). Nigerians are known both home and abroad to be rampant perpetuators of cybercrimes. The numbers of Nigerians caught for duplicitous activities carried by broadcasting stations are much more in comparison to other citizens of different countries. The contribution of the internet to the development of Nigeria has had a positive impact on various sectors of the country. However, these sectors such as the banking, e-commerce and educational sector battles with the effect of cybercrimes. More cybercrimes are arising at an alarming rate with each subsequent crime more advanced than its predecessor. Therefore, in this section, prominent specific ways in which cybercrimes are mostly carried out in Nigeria are discussed the life wire of the banking sector is the internet. Currently, banks all over the world are taking advantage and incorporating opportunities brought about by e-banking which is believed to have started in the early 1980's (Shandilya, 2011). As the security level in this sector becomes stronger, the strength and tactics of these fraudsters increases also. Various lucrative attacks have been launched and unfortunately, many have succeeded. In general, cybercriminals execute fraudulent activities with the ultimate goal of accessing a user's bank account to either steal or/and transfer funds to another bank account without rightful authorization. However, in some rare cases in Nigeria, the intention of cyber-criminals is to cause damage to the reputation of the bank by denying service to users (Parthiban, 2014) and sabotaging data in computer networks of organizations. Bank Verification Number (BVN) Scams: The BVN is a biometric identification system which consists of an 11-digit number that acts as a universal ID across all the banks in Nigeria. BVN was implemented in 2015 by the Central Bank of Nigeria. It was introduced to link various accounts to the owner thereby ensuring that fraudulent activities are minimized. For fraudsters, opportunities to extort money and to carry out other fraudulent activities arose from the implementation of the BVN. It was detected that fake and unauthorized text messages and phone calls were sent to various users demanding for personal information such as their ac-count details. In addition, phishing sites were created to ac-quire such information for insalubrious activities on the bank account. Phishing: Phishing is simply the theft of an identity. It involves stealing personal information from unsuspecting users and it is also an act of fraud against the authentic, authorized businesses and financial institutions that are victimized (Wada). Phishing scams are ubiquitous and are exponentially increasing. It has become one of the fastest growing cybercrimes in Nigeria. In this jet age of technology, hoi polloi subscribe to a plethora of sites using their email ad-dresses and are therefore expecting to receive mails of updates of their membership or subscription. So it seems natural when users get regular mails from such organizations. Fraudster have devised a means to mimic authorized organ

## Cases of Cybercrimes Globally

### *The telegraph system*

In 1834, two thieves infiltrated the French telegraph system, gained access to financial markets, and stole data. Many experts consider this event the first cybercrime, followed by other cybercrimes, each focusing on newly invented technologies.

### *The telephone system*

The 19th and 20th centuries saw attacks focused on the telephone system. In 1876, Alexander Graham Bell patented the phone, which allowed transmitting speech using telegraphy. Two years after the commercialization of this invention, teenage boys broke into Bell's telephone company and misdirected calls. In later years (1960s-1980s), phone hacking (phreaking) became popular.

### *Ethical hacking*

In 1940, Rene Carmille, a French computer expert, hacked into the Nazi data registry. Carmille, a punch card computer expert, used his expertise to reprogram Nazi punch card machines to prevent them from registering information correctly. His work blocked the Nazis' attempts to register and track Jewish people.

### *Phishing scams and malware*

In the 1980s, emails became a popular communication form, and by the 1990s, web browsers and computer viruses rose in popularity. In these years, hackers started using email attachments to deliver malware and phishing scams and web browsers to spread computer viruses.

### *Social media scams*

Social media networks gained worldwide popularity in the 2000s, and hackers started utilizing these platforms for data theft and other cybercrimes. In the following years, cybercriminals improved malware infections and data theft techniques. Today, these attacks are deployed in the thousands, constantly increasing with no signs of slowing down.

### *Hacking the Internet of Things (IoT)*

IoT has provided cybercriminals with a wealth of hacking opportunities. IoT technology upgrades ordinary objects, like washing machines, refrigerators, light bulbs, and heating systems, with Internet capabilities. Since these devices are connected to the Internet, cybercriminals can hack into them and cause damage that extends to the physical world.

## Danger of Cybercrime

According to Cram.com (2023) The impact of technology and networks on our lives, culture, and society will continue to increase. The advancement in technology has also led to the growth of cyber-attacks. As with most crimes that are committed, money seems to remain a major motivator. Most cyber criminals or hackers feel a little more secure when they can hide behind a network; the perception of low risk and very high financial reward prompts many cyber criminals to engage in malware, phishing, identity theft, and fraudulent money request attacks.

Today all significant businesses in all industries depend on technology and data systems. Recent shifts to cloud-based environments, interoperability, data sharing, and the use of multiple apps to conduct daily business, impose an inherent risk of cybersecurity issues such as active threats, data theft, data loss and ransomware demands. The risk has been compounded by the pandemic, exposing vulnerabilities associated with migration to remote working environments. Last year, cybercrime became more expensive. Data breach costs increased from $3.86M in 2020 to $4.24M in 2021 per organization breached. COVID-19 had a negative impact too; the average cost of a breach was $1.07M higher when remote work was a root factor, compared to when it wasn't, (Sanjaya Kumar2022)

Cyber criminals seek to exploit human or security vulnerabilities in order to steal passwords, data or money directly. The most common cyber threats include:

- Hacking - including of social media and email passwords
- Phishing - bogus emails asking for security information and personal details
- Malicious software – including ransomware through which criminals hijack files and hold them to ransom
- Distributed denial of service (DDOS) attacks against websites – often accompanied by extortion. ( National crime agency 2023).

## Concept of Cyber Resilience

According to Cassim (2011), the concept of cyber resilience underlines the need for broad, concerted and comprehensive approaches to cyber security, but in reality, the implementation of measures to curb cyber attacks has been selective and driven by narrower agendas. Cyber resilience refers to an entity's ability to continuously deliver the intended outcome despite adverse cyber events and that with it risk is certainly reduced (Howell and Lind, 2009). Ploch (2010) assert that cyber resilience is an evolving perspective that is rapidly gaining recognition. The concept essentially brings the areas of information security, business continuity and (organizational) resilience together. Entities with potential need of cyber resilience abilities include; IT systems, critical infrastructure, business processes, organizations, societies and nation-states. Adverse cyber events are those that negatively impact the availability, integrity or confidentiality of networked IT systems and associated information and services. These events may be intentional (e.g. cyber attack) or unintentional (e.g. failed software update) and caused by humans or nature or a combination thereof (Greenwald, 2014).

As stated by Akpan (2019????) the objective of cyber resilience is to maintain the entity´s ability to deliver the intended outcome continuously at all times. This means even when regular delivery mechanisms have failed, such as during a crisis and after a security breach. The concept also includes the ability to restore regular delivery mechanisms after such events as well as the ability to continuously change or modify these delivery mechanisms if needed in the face of new risks. Backups and disaster recovery operations are part of the process of restoring delivery mechanisms. The objective is therefore maintaining as much normalcy as possible or returning to that level as quickly as possible following a cyber attack (Stremlau and Osman, 2015). Resilience, as defined by Presidential Policy Directive PPD-21, is the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Cyber resilience focuses on the preventative, detective, and reactive controls in an information technology environment to assess gaps and drive enhancements to the overall security posture of the entity.

The African Union Convention on Cyber Security and Personal Data Protection, which offers continental reference to improve cyber preparedness in Africa, has also raised concerns that in the charged political climate characterizing many countries on the continent, the heightened emphasis on security and state-led responses may impact free speech and privacy as governments that have been criticized for their abuses gain enhanced abilities to police the cyber world (Macharia, 2014). The possibility that personal data could be processed without subjects giving free and informed consent delineate scenarios where users may be stripped of their ability to be in control of their data and, on the contrary, be controlled in the name of agendas they had little voice in shaping (Access, 2014).

## Concept of Cyber Security

Ravi (2003) asserts that cyber security is the protection of systems, networks and data in cyberspace and is essential even as more people get connected to the internet across the world. The International Telecommunications Union [ITU] defines Cyber security as "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."

The ITU also notes that the three broad security objectives are ensuring Availability; Integrity (which may include authenticity and non-repudiation), and Confidentiality. While these are the bedrock of a secure network, achieving these three objectives is no mean feat as it requires the integration of various functions such as robust systems engineering and configuration management; effective cyber security or information assurance policy and comprehensive training of personnel. Cyber security 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 internet (Steffani, 2006). Cyber Security can also be described as the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access (Thilla, 2012).

## Concept of Cyber Risk

Cyber risk can be defined as the risk connected to activity online, internet trading, electronic systems and technological networks, as well as storage of personal data. According to Deloitte Advisory Cyber Risk Services (2013), the fundamental things that organizations undertake in order to drive performance and execute on their business strategies happen to also be the things that actually create cyber risk. This includes globalization, mergers and acquisitions, extension of third-party networks and relationships, outsourcing, adoption of new technologies, movement to the cloud, or mobility.

Cyber risk is an issue that exists at the intersection of business risk, regulation, and technology. Events covered by this more comprehensive definition can be categorized in multiple ways. One is intent. Events may be the result of deliberately malicious acts, such as a hacker carrying out an attack with the aim of compromising sensitive information, but they may also be unintentional, such as user error that makes a system temporarily unavailable (www.reuters.com). Risk events may come from sources outside the organization, such as cybercriminals or supply chain partners, or sources inside the organization such as employees or contractors. Combining these two dimensions leads to a practical framework for inventorying and categorizing cyber risks into:

Internal Malicious: Deliberate acts of sabotage, theft or other malfeasance committed by employees and other insiders. For example, a disgruntled employee deleting key information before they leave the organization.

## Strategies to Strengthen Cyber Security and Cyber Resilience

Based on the World Economic Forum (2012) research findings, most Nigerian organisations are ill-equipped to respond to information security threats. Although there are different initiatives (regulators, government and private organisations) in place set out to address information security issues in Nigeria, these initiatives cannot adequately address the current information security issues. Public and private organisations need to rethink their whole approach to information security and establish security practices needed to protect critical IT infrastructure. They also need to train and grow security experts needed to secure this infrastructure. Most organisations now recognize that it is imperative that local organizations take action before the situation worsens and the cost of inaction becomes even greater (World Economic Forum, 2012).

Lamorde (2015) maintained that just as it is with the European Union, North America and several countries in Asia have come up with National Strategy on Cyber security. The Nigerian National Cyber security framework should consider internet security as vital to a vibrant digital society. It should set out action plans to improve cyber security readiness and provide response and management of breaches for all internet users.

Lamorde (2015) suggested that the strategy should include the establishment of a well-functioning network of Computer Emergency Response Team at the national level. The organisation of cyber incidents simulations, putting in places a well-defined policy on Critical Information Infrastructure Protection (CIIP) with the aim of strengthening the security and resilience of ICT Infrastructure. He advised that in order to ensure a safer internet for our kids and young persons, the framework should create a strategy that will provide a safer and more secured cyber space for our young ones.

Juwah (2015) assert that countries need to step up; work together to build and provide information security services that enables Nigeria to address these challenges. Nigerians need to leverage their local presence and understanding of the environment to provide a clear indication of the security problems on the ground. This local presence combined with partnerships with regional and global players will provide globally tested solutions and approaches to address identified security problems.

According to Akpan (2019???) mostly used strategies in strengthening Cyber Security and Resilience against Cyber Risk in Nigeria was the that "The organisation of cyber incidents simulations, putting in places a well-defined policy on Critical Information Infrastructure Protection (CIIP)”

He also noted that Cyber Security and Cyber Resilience have helped in reducing cyber risk in Nigeria to very high extent. According to Akpan (2019??) his survey result proved that there is significant difference in the perception of people as regards the effect of cyber security and cyber resilience in reducing cyber risk in Nigeria. In his conclusion he stated that Nigeria as can be found in other part of the world, has suffered greatly in Cyber-attack and that cyber security and resilience has become useful tool to checking and stopping cyber risks and with Cyber security and resilience our society is protected against cyber risk.

## Conclusion

The study concludes that the alarming growth of the internet and its wide acceptance has led to increase in security threats. In the world today, including Nigeria several internet assisted crimes known as cybercrimes are committed daily in various forms such as fraudulent electronic mails, pornography, identity theft, hacking, cyber harassment, spamming, Automated Teller Machine spoofing, piracy and phishing. Cyber security is one of the great human rights issues of our time. The cyber security has helped in reducing cyber risk in Nigeria to a very high extent.

## Recommendations

1. Countries should build upon the work of the Global Community Engagement and Resilience Fund (GCERF) which supports local, community-level initiatives aimed at strengthening resilience against cyber attacks.

2. Organizations should build awareness of security issues across the internet community and promote cyber security awareness.

3. To improve cyber security posture over the years, companies should invest in enabling technologies and staffing.

4. Public and private organizations need to rethink their whole approach to information security and establish security practices needed to protect critical IT infrastructure.

## REFERENCES

Access, A. (2014). *African Union Adopts Framework on Cyber Security and Data Protection*. www.accessnow.org/blog/2014/08/22/african-union-adopts-frameworkon-cyber-security-and-data-protection.

Adepetun, A. (2020) Cyber attack on Nigerian SMEs up by 89 per cent in 2022. Available at: https://guardian.ng/business-services/cyber-attack-on-nigerian-smes-up-by-89-per-cent-in-2022/

BlueVoyant, (2023) *Cybercrime: History, Global Impact & Protective Measures.* Retrieved from: https://www.bluevoyant.com/knowledge-center/cybercrime-history-global-impact-protective-measures-2022

Cassim, F. (2011) *Addressing the growing spectre of cyber crime in Africa: evaluating measures adopted by South Africa and other regional role players.* CILSA XLIV 123-138

Climer, S. (2018) *History of Cyber crime From the Morris Worm to Exactis*. Available at: https://gomindsight.com/insights/blog/history-of-cyber-attacks-2018/

Cram.com (2023) Dangers Of Cybercrime. Retrieved from: https://www.cram.com/essay/Dangers-Of-Cybercrime/PJYCBY25YR6

Deloitte Advisory Cyber Risk Services (2013) *Information Security*: A Strategic Approach. IEEE Computer Society, Hoboken, NJ.

Editorial (2022) The CBN Cybercrimes Framework Available at: https://www.thisdaylive.com/index.php/2022/07/18/the-cbn-cybercrimes-framework/

Governance (2015) *Cybersecurity Strategy*. Ministry of Information Communications and Technology

Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York, NY: Metropolitan Books/Henry Holt.

Howell, J. & Lind, J. (2009). *Counter-Terrorism, Aid and Civil Society: Before and After the War on Terror*. Basingstoke, UK: Palgrave Macmillan. ISACA, 2014).

Juwah, M. (2015) *Returns to information security investment: the effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability.* Information System Front 8 (5), 339–349.

Kaplan, B., James, D. and Tucker, N. (2015) Theory of deterrence and individual behavior. Can lawsuits control file sharing on the Internet? *Review of Law and & Economics* 3 (3), 693–714.

Lamorde (2015) Education, poverty, political violence, and terrorism: is there a connection? *Journal of Economic Perspectives* 17 (4), 119–144.

Macharia, D. (2014) Theory of deterrence and individual behavior. Can lawsuits control file sharing on the Internet? *Review of Law and & Economics* 3 (3), 693–714.

Mihir Bagwe (2022) Nigerian Police Bust Gang Planning Cyberattacks on 10 Banks Available at: https://www.bankinfosecurity.com/nigerian-police-bust-gang-planning-cyberattacks-on-10-banks-a-19320

National crime agency (2023) Cyber crime. Available at: https://www.nationalcrimeagency. gov.uk/what-we-do/crime-threats/cyber-crime

Omodunbi, B., Odiase, P., Olaniyan, O. & Esan, A.( 2016) Cybercrimes in Nigeria: Analysis, Detection and Prevention. Retrieved from: https://www.researchgate.net /publication/320411102_Cybercrimes_in_Nigeria_Analysis_Detection_and_Prevention

Perlroth, G. & Nicole, E. (2016) Perlroth, Nicole, *Hackers use new weapons to disrupt major webites across U.S*, The New York Times, 21 October http://www.nytimes.com /2016/10/22/business/internet-problems-attack.html

Ploch, D. (2010) *The Information System and the Global Terrorism*. SSRN: <http://www.ssrn.com/abstract=906289> (retrieved 2008).

Ravi, D. (2012) How optimal penalties change with the amount of harm. International *Review of Law and Economics* 15 (1), 101–108.

Ravi, V. (2003) Toward an integration of criminological theories. *Journal of Criminal Law and Criminology* 76 (1), 116–150.

Sanjaya Kumar (2022) Cybercrime: A clear and present danger. Retrieved from: https://www.securitymagazine.com/articles/97190-cybercrime-a-clear-and-present-danger

Schneier, D. & Bruce, C. (2016). *Lessons From the Dyn DDoS Attack*, Schneier on Security Blog, 8 November 2016, https://www.schneier.com/blog/ archives/2016/11/lessons_ from_th_5.html

Schubert, J. (2022) *what is Cybercrime? - Definition, History, Types & Laws*. Retrieved from: https://study.com/academy/lesson/what-is-cybercrime-definition-history-types-laws.html

Shola Soyele (2020) EFCC Arrests Two Music Producers Over Alleged Cyber Crimes In Uyo. Retrieved at: https://www.channelstv.com/2020/09/12/efcc-arrests-two-music-producers-over-alleged-cyber-crimes-in-uyo/

Soonest Nathaniel (2021) Police Cybercrime Centre Arrests Two For Computer-Related Fraud. Available at: https://www.channelstv.com/2022/12/29/police-cybercrime-centre-arrests-two-for-computer-related-fraud/

Steffani, H. (2006). Do bad boys really get the girls? Delinquency as a cause and consequence of dating behavior among adolescents. *Justice Quarterly* 21 (2), 355–389.

Stremlau, D. & Osman, E. (2015) *A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behavior*: An Exploratory Study. University of Manitoba, Winnipeg, Manitoba.

Thilla, D. (2012) The economics of crime and punishment: an analysis of optimal penalty. *Economics Letters* 68 (2), 191–196.

Thomas, T., Karas, D., Lori, P. & Parrott, D. (2008) A framework for predicting security and dependability measures in real-time. *International Journal of Computer Science and Network Security* 7 (3), 169–183.

Uche Igwe (2021) Nigeria's growing cybercrime threat needs urgent government action. Retrieved from: https://blogs.lse.ac.uk/africaatlse/2021/06/09/nigerias-growing-cybercrime-phishing-threat-needs-urgent-government-action-economy/

Vanson, H. & Bourne, M. (2012) A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency* 34, 495–518.

Wiley,D. (2015) Towards cost-sensitive modeling for intrusion detection and response. *Journal of Computer Security* 10 (1–2), 5–22.

World Economic Forum (2012) *Convergence on the outcome economy*, http://reports.weforum.org/industrial-internet-of- things/3-convergence-on-the-outcome-economy/3-2-the-emergence-of-the-outcome economy/?doing_wp_cron=1463567483. 8225409984588623046875