INTERNATIONAL JOURNAL OF ARTS MANAGEMENT AND PROFESSIONAL STUDIES
E-ISSN: 2814-0389, ISSN: 2814-0370
VOL. 5, ISSUE 1, 2025
AVAILABLE ONLINE: www.ijamps.com

Cybersecurity: Threats and Challenges in Nigeria

Eze Chidi Nwauba
Professor of Intrapreneurship
Department of Public Administration,
Prowess University, Delaware-USA
E-mail: dparlay@gmail.com
dr.prince@pu-edu.us
+2349124673109
+22996547204

Abstract

All that limitless expanse of the internet is called cyber-space. A set of cyber-security regulations has been established to safeguard the cyber domain. Attacks on cyberspace and cybersecurity are collectively known as cyber-crime. Few sectors of the technological infrastructure are expanding at a faster rate than the Internet. This option has been made available to everyone over the past few decades due to the proliferation and usage of the internet. Millions of people daily rely on search engines like Google, Wikipedia, and Bing to get thorough answers to their questions. In cyberspace, one may find practically everything they are looking for. The proliferation of cybercrime is a direct result of the proliferation of online information and the many benefits and uses of the internet. The necessity to address cyber security threats more seriously has propelled the issue to the level of a national priority.An outline of cybercrime and cybersecurity is the goal of this paper. It explains what cybercrime is, the factors that contribute to it, and strategies for eliminating it. The people involved, and the circumstances surrounding their involvement are examined. The paper focused on improving cyber security and offered suggestions to slow the growing number of cybercrimes. Also, the study tries to identify some problems with cybercrime and provide some reasonable and realistic ways to fix them.

Keywords: ICT, DOC, NCI, NCWG, Cybercrime, Cybersecurity

Introduction

In a real-time processing mode, the internet has eased business activities like sorting, summarizing, coding, editing, and the development of both generic and customized reports for businesses, industries, governments, and non-profits. Unforeseen effects include an increase in spam, credit card and ATM fraud, phishing, identity theft, and criminal activity. Cybercrime has also flourished as a result of the Internet (Anderson et al., 2012). Cybercrime is a new kind of conflict that, if left unchecked, threatens to wreak more havoc than the two global wars that came before it. This study aims to depict a scenario of its emergence. It is well-known that Nigeria is a very receptive nation. For her, there were many benefits and drawbacks to the rise of the internet. Nigeria has recently experienced a shocking surge in cybercrime, which has had a devastating effect on the country's economy and society (Adebusuyi, 2008).

While the general public has experienced a range of emotions—from admiration to fear—in response to the persistence of immoral Internet users over the past two decades, there has been an increasing sense of anxiety regarding the status of cyber and personal security (Longe & Chiemeke, 2008). There has to be swift action in passing legislation to safeguard cyberspace and its users because this phenomena has recently witnessed a sophisticated and unprecedented upsurge.

It was seven years ago in the US that the first cyber murder was documented. A minor operation was scheduled for an underworld don in a hospital, according to the Indian Express (January 2002). A computer expert that his adversary hired changed his prescriptions by hacking into the hospital's computer system. An unsuspecting nurse gave him the patient's changed prescription, and the patient died. From 2006 forward, every single day has seen some sort of cybercrime worldwide (Adebusuyi, 2008). Worldwide, the term "cybercrime" was not used to describe Nigeria until 2001. This jives with the fact that around the same time, we in Nigeria began to fully appreciate the internet's capabilities. But since then, the nation has become notorious all across the globe for illegal activities, particularly online financial scams (Odinma, 2010).

The tools used to monitor these criminals have become outdated due to the fact that Nigerian cybercriminals are constantly coming up with new ways to commit this type

of crime. Victims also display a growing degree of gullibility and innocence when it comes to the opportunities enticed by these con artists (Adebusuyi, 2008). Given that Nigerians are understandably curious about cyber security, it is only right that we address their concerns. Cybercrime and cybersecurity are broad topics, and this paper will try to cover them fully, as well as highlight certain problems and possible solutions.

Literature Review

Many people, each with their own unique viewpoint on the matter, have spoke about cybercrime and its many facets. Even for highly technologically advanced nations like the US, cybercrime has expanded beyond traditional criminal activity and now poses a danger to nation security (Anderson et al., 2012). "The adoption by all countries of appropriate legislation against the misuse of Information and Communication Technology (ICT), for criminal or other purposes, including activities intended to affect the integrity of national critical information infrastructures, is central to achieving global cyber security," (Longe & Chiemeke, 2008). According to Odinma (2010), international cooperation, investigative aid, and uniform substantive and procedural provisions are necessary because the challenges are intrinsically global in scope and potentially originate anywhere in the world. Consistent with the foregoing, Professor Augustine Odinma defines cybercrime as "any illegal acts perpetrated in, on or through the internet with the intent to cheat, defraud or cause the malfunction of a network device, which may include a phone, a computer, etc.." Instances of computer viruses, denial of service attacks (DOS), and malware are examples of criminal acts that target computer networks or devices (Odinma, 2010). An unauthorized conduct can be made easier with the use of a computer network or device, even while the intended victim is unrelated to the technology. In a paper demonstrating his interest in the country's military, Major General Umo ties cybercrime to the military and states that cyberterrorism, cyberwarfare, and cybersecurity are converging concepts. Why? Because committing an act of theft or forgery with the intent to harm a specific person or entity is the same as declaring war on that target (Longe & Chiemeke, 2008).

As far as cybercrime goes, Nigeria ranks third in the globe and 43rd in EMEA (Olumide & Victor, 2010). Back in 2003, Nigeria's then-president Olusegun Obasanjo established the National Cyber Security Initiative (NCI) to address the issue. Despite the Nigerian Cybercrime Working Group's (NCWG) best efforts, the results of NCI's goals have lagged behind the exponential expansion of cybercrime. Professor Oliver Osuagwu draws attention to the fact that ninety percent of cybercriminals originate from the education sector, which is leading to the near-total collapse of the education community, especially in Nigeria. One of the main causes of cybercrime in Nigeria is the wrong value system (Strassmann, 2009), which encourages people to want to get rich fast. The complexity and geographical dispersion of cybercriminals make it harder to crack down on this type of crime. It is already difficult for police to do their jobs without an enabling statute (Olumide & Victor, 2010).

As mentioned before, there are more positive than negative things that can happen on the internet. What Mrs. R. Moses Oke means when she says in Moses-Òkè (2012) that "the oxymoronic nature of the Internet is one of its unforeseen attributes" is that no one could have predicted when the Internet was first created that it would become a platform for crimes all over the world. Numerous people have pointed out that the Internet's usefulness has been tarnished by the fact that it may be used for illegal actions, which have significant negative effects on society and the environment. Many would agree that worries are growing as Nigeria continues to digitize its economy, communications, and, slowly but surely, its electronic banking systems. According to Longe & Chiemeke (2008), much attention has been paid to electronic banking and the cashless effort in the last few years.

According to an article by Amaka Eze published in THISDAY live, "as the country integrates electronic payment system into its financial institution; a step that is expected to accelerate the nation‟s e-commerce growth, the negative impact of cybercrime on businesses and the absence of appropriate laws to guarantee the legality of online transactions, continue to create fear in the mind of users and potential online users (Amaka Eze, n.d.)." Despite the fact that cybercrime and breaches in cyber- security are on the rise and pose serious threats, the focus should be on finding solutions to lower or eliminate their occurrence in Nigeria. The people

concerned must invest effort into understanding the inner workings of cybercrime rings in order to formulate countermeasures and bring cybersecurity back to its former glory (Schaeffer et al., 2009). Using technology from the past will not be effective in opposing modern crimes. When defensive experts lack the technological expertise of cybercriminals, the fight against cybercrime is doomed to fail (Longe & Chiemeke, 2008). Expertise in IT security is equally as important as proficiency in programming.

Costs to the government as a result of cybercrime's upsurge have also been covered earlier. According to the Detica report in International Telecommunication Union (n.d.), there are four ways to measure the costs of cybercrime: the costs that companies incur before the crime even happens, like antivirus software, insurance, and compliance; the costs that happen as a result of the crime, like direct losses and indirect costs like weakened competitiveness due to intellectual property compromise; the costs that companies pay as a response to the crime, like compensation to victims and fines to regulatory bodies; and the indirect costs, like reputational damage to firms, loss of confidence in cyber transactions by individuals and businesses, reduced public-sector revenues, and the mushrooming underground economy (Olumide & Victor, 2010). Now that we have considered cybercrime from a variety of angles, we can go headfirst into a discussion of cybercrime and cybersecurity, complete with real-world examples and tools for resolving the issue. Although law enforcement has made significant strides, cybercrime continues to be carried out by unseen persons.

Cybercrime and Cybersecurity: A High-Level Review

Cyberspace, cybersecurity, and cybercrimes have all evolved in meaning alongside the expansion of digital technology. Some have stated that in order to define computer crime, the focus should be on the specificity, the understanding, or the use of computer technology, as this type of crime might encompass all others. The infinite void that is the internet is referred to as cyber-space (Anderson et al., 2012). Many of our current communication technologies are based on this complex web of interconnected information and communication networks. Protecting the cyber environment and the assets of organisations and users can be achieved through cyber security, which is a compilation of various tools, policies, security concepts, safeguards, guidelines, risk management techniques, activities, training, best practices,

assurance, and technology (Strassmann, 2009). Cyber assets encompass any information that is transported or stored in the cyber environment, as well as connected computing equipment, personnel, infrastructure, applications, services, and telecommunications systems (Background Check International, n.d.). Ensuring the protection of an organization's and user's assets from potential security threats in the cyber environment is the major goal of cybersecurity (International Telecommunication Union, n.d.), Cyber-security refers to the set of regulations designed to keep the internet safe. The more reliant we are on the internet, the more dangers there will be. When a group of criminals launch coordinated attacks on cyberspace and cyberdefense, they are committing cybercrime. There are a lot of threats to our economy and national security, including nation-states and highly skilled cybercriminals. Cyberspace encompasses an extensive web of interconnected and vital networks, systems, services, and resources that are essential to the economic growth and national security of Nigeria (Oliver, 2010). Our ability to communicate, travel, power our houses, manage our economy, and access government services has all been revolutionised by cyber-space.

To prevent harm, damage, or unauthorised access to computer networks, data, programmes, and programmes, cyber-security encompasses a wide range of technologies, procedures, and policies. The term "security" simply means "Cyber-security" when used in a computer or cyber setting (International Telecommunication Union, n.d.). It takes joint endeavours from the nation's inhabitants and its information system to guarantee cyber-security. Cybersecurity threats are evolving at a rate that outpaces our ability to respond. It would be irresponsible to ignore or ignore the other parts of the breach in favour of focusing on just one. So, it is clear that we need to take a comprehensive approach to addressing cyber-security breaches. So, what exactly are these violation?

Cyber-crime encompasses illicit activities conducted using computers and the Internet. This encompasses a wide range of activities, ranging from illicitly acquiring copyrighted music files to embezzling substantial sums of money from internet financial institutions (International Telecommunication Union, n.d.). Cybercrime include nonmonetary offences, such as the creation and dissemination of computer

viruses or the unauthorised disclosure of confidential company information over the Internet. Identity theft is the most prevalent type of cybercrime, where criminals exploit the Internet to unlawfully obtain personal information from other individuals (Anderson et al., 2012). The most comprehensive definition of cybercrime is as follows: Cybercrime refers to illegal activities carried out using information technology infrastructure. These activities include unauthorised access, which involves gaining entry to a computer system without permission. It also includes illegal interception, which involves using technical means to intercept non-public transmissions of computer data (Background Check International, n.d.). Data interference refers to unauthorised actions that damage, delete, deteriorate, alter, or suppress computer data. Systems interference involves disrupting the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data. Other forms of cybercrime include the misuse of devices, forgery (such as identity theft), and electronic fraud (Oliver, 2010).

Cyber Security Objectives

It is the goal of cyber-security to accomplish the following:

- To assist individuals in making their ICT systems and networks less susceptible to attacks.
- To assist both individuals and organisations in fostering a cyber security culture.
- To secure cyberspace through joint efforts with public, commercial, and international organisations so that we can comprehend the present tendencies in IT/cybercrime and create efficient remedies.
- To be available.
- Integrity includes being trustworthy, being unable to dismiss or downplay any evidence, and keeping data secure.

Online Crimes that are Unique to Nigeria

Nigeria has suffered severe image trauma due to e-crime. The nation is deeply troubled and humiliated by cybercrime. The Internet opens up boundless social, educational, and commercial possibilities. Cybercrime, however, shows that the Internet also has its own unique dangers. From the most prominent online scams to phoney lotteries, it is everything here. Despite possessing a degree in computer

technology, 28-year-old chubby-faced Elekwe was unemployed for two years before he became wealthy through the hoax. From Umuahia, he was enticed to Lagos by the head of a fraud ring in a commercial centre. Through his adventures, he has amassed three stylish automobiles and two residences. Security services in Ghana apprehended four Nigerians in July 2001 on suspicion of running an online "419" scheme to defraud naive overseas investors. Potential investors reportedly lost millions of dollars worth of foreign currency due to their actions. A woman's website falsely offered two laptops, and two young males were detained for making the deal. Officials from the authorities apprehended them when they were being delivered. Mike Amadi received a 16-year prison term for creating a website that advertised lucrative but fraudulent procurement contracts. An undercover agent pretending to be an Italian businessman apprehended the individual who had assumed the identity of the EFCC Chairman. Amaka Anajemba, sentenced to 2½ years in prison, conducted the largest international swindle ever. In addition, she was directed to repay $25.5 million out of the $242 million that she assisted in embezzling from a bank in Brazil (Schaeffer et al., 2009).

A 24-year-old woman named Yekini Labaika from Nigeria's Osun State and a 42-year-old American nurse named Thumbelina Hinshaw were both involved in an online fraud alleging a Muslim lover looking to get married. The story was published in the Sunday PUNCH newspaper on July 16, 2006. A young man named Phillip Williams pretended to be an American Muslim who was working for an oil firm in Nigeria when he tricked the victim into believing he was her future husband. He used shady tactics to con the victim out of $16,200 and a plethora of precious items. Following his conviction on eight counts, the con artist received a sentence of nineteen and a half years in prison. These kinds of incidents are becoming more common. The criminal activities of a handful of young men who prey on naive individuals and organisations continue unabated (Oliver, 2010). A recent study estimated that software piracy costs Nigeria almost $80 million annually. Business Software Alliance of South Africa commissioned the research from the South African market research and forecasting business Institute of Digital Communication, which produced the report (Schaeffer et al., 2009). According to the American National Fraud Information Centre, Nigerian money promises were the most rapidly expanding

type of internet fraud in 2001, with a growth rate of up to 90%. According to the Centre, the impact of cybercrime per capita in Nigeria is extremely large (Anderson et al., 2012).

People primarily residing in urban centres between the ages of 18 and 25 are involved. The internet has played a role in bringing young people's fraudulent behaviours into the modern era. The teenagers participating view online fraud as a widely accepted way to support themselves financially. A subculture of computer criminals has flourished due to the corrupt political leadership (Olumide & Victor, 2010). A big component in the engagement of young people in internet fraud is the importance put on accumulating cash.

Classifications of Cybercrime

Hacking: When hackers break into a computer system, they look for security flaws and vulnerabilities that they can exploit to steal sensitive information or corrupt data. The most common method is installing a backdoor programme on your computer. Password hacking software is another common tool hackers employ to access resources (International Telecommunication Union, n.d.). Additionally, hackers can spy on your online activity and even steal files from your computer. An intruder could secretly install multiple programmes on your computer. Passwords and credit card details are only some of the personal information that could be stolen by such programmes (Strassmann, 2009). It is also possible to hack into a company's critical data to learn its secret strategies for the future.

Cyber-Theft: Theft of data stored electronically through the use of computer networks and other forms of electronic communication is known as cyber-theft. Criminals with hacking skills get unauthorised access to financial institutions' networks and steal funds for personal use. Since higher sums of money can be taken and transferred illegally, this is a big worry. One more prevalent kind of fraud is credit card fraud. For fear of alienating consumers and shareholders, most businesses and financial institutions keep quiet about having been victims of cyber-theft (Background Check International, n.d.). Out of all cybercrimes, cybertheft receives

the most attention and reports. One of the most common forms of cybercrime, cyber-theft allows skilled cybercriminals to easily amass substantial sums of money with no effort.

Viruses: Worms and viruses pose a significant risk to both individual users and businesses. Intentionally harmful computer programmes are known as viruses. Because it replicates itself in the same way that biological viruses do, this programme is called a virus (Schaeffer et al., 2009). In order for a virus to infect a computer, it must be connected to another programme or document. Worms typically take advantage of security flaws in software or the OS. Using a Trojan horse has its risks. Although it seems to do one thing, it actually does something different. Perhaps the system will treat it as a single item. A logic bomb, virus, or worm might be released while it runs (Background Check International, n.d.). An assault known as a logic bomb occurs when a predetermined event occurs, such as a computer clock reaching a specified date. Recent instances include the Melissa virus and the Chernobyl disaster. On a single day in January 2004, the Mydoom worm infected almost 25,000 systems, according to experts. For the duration of March 1999, Microsoft and other major corporations were compelled to disable their email systems entirely due to the formidable Melissa virus. This measure was taken in order to contain the infection.

Spamming: Sending out an overwhelming number of promotional emails to promote and market websites and products is known as spamming. Businesses are increasingly facing the problem of email spam, which is causing significant costs in terms of bandwidth use and the time spent downloading and removing spam messages (Oliver, 2010). Additionally, spammers are getting better and better at evading spam filters by doing things like using images that spam systems cannot identify and randomly rearranging the text of emails.

Financial Fraud: Financial fraud, sometimes known as "Phishing" scams, requires the criminals to pretend to be a reliable official from a company (Schaeffer et al., 2009), most often the victim's bank, and involves some form of social engineering.

Identity Theft, Credit Card Theft, Fraudulent Electronic Mails (Phishing): Phishing is the practice of sending an email that appears to be from a well-known, genuine company in an attempt to trick the recipient into divulging sensitive information that can be utilised for fraudulent purposes, such as identity theft.

Cyber Harassment: The term "cyber harassment" refers to the practice of threatening someone using electronic means with the purpose to do harm. One example of this is cyberstalking.

Cyber Laundering: The transfer of illicitly acquired funds through electronic means with the intention of concealing both their origin and their ultimate destination is known as cyber-laundering.

Website Cloning: A current trend in cybercrime involves the rise of counterfeit websites that exploit consumers unfamiliar with the Internet or who do not know the precise web URL of the legitimate organisation they intend to see. The consumer, under the false impression that they are inputting their credit information to make a legitimate purchase from the intended company, is unknowingly providing their details to a fraudster's database (Moses-Òkè, 2012). Subsequently, the swindler can utilise this information later for personal gain or to vend to those interested in committing credit card fraud.

Contemporary Online Scams in Nigeria

i. **Beneficiary of a Will Scam:** In this scam, the perpetrator uses email to pretend to be a distant relative's appointed beneficiary, giving the victim the chance to inherit a multimillion-dollar estate.

ii. **Online Charity:** Another kind of e-crime prevalent in Nigeria is imposters posing as legitimate nonprofits over the internet to steal money and supplies. Such tactics have, alas, taken advantage of many naive individuals.

iii. **Next of Kin Scam:** Scam artist extorts victims out of millions of dollars in a Nigerian bank they believe a long-lost relative left them, along with transfer fees and other funds.

iv. **The "Winning Ticket in Lottery you Never Entered" Scam:** The green card lottery run by the State Department is one of the recent scams.

v. **Bogus Cashier's Check:** A person contacts the victim after seeing an online ad for a product they are selling.

vi. **Computer/Internet Service Time Theft:** Geeks in Nigeria have come up with a way to link cyber cafes to the networks of some internet service providers (ISPs) in a way that the ISPs would not notice, so the cafes can run on free internet.

vii. **Lottery Scam:** pretending to be an online lottery that fools users into thinking they won.

Cybercrime: Emerging Challenges

• The rate of electronic crime in Nigeria has surpassed that of Internet usage, according to Tunji Ogunleye, a consultant specialising in information and communication technology security and a member of the Nigeria Cyber Crime Working Group (NCWG). In terms of Internet usage, Nigeria ranks 56th out of 60 countries, according to him, but third when it comes to scam attempts. Maybe we should inquire as to the causes of the recent spike in cybercrime in Nigeria and the characteristics that have rendered Nigerians so susceptible to this kind of crime.

• An adversary located thousands of kilometres away can just as easily launch an attack on Nigerian internet-connected machines as if he were sitting next door, which poses a threat to both local and international law enforcement (Schaeffer et al., 2009). Criminal prosecution across national boundaries is complicated, and identifying the perpetrator of such an incident is often difficult.

• Among the most concerning issues is the alarmingly high rate of unemployment in Nigeria. Many banks and businesses are declaring bankruptcy recently. It has been suggested by the federal government that government employees be mass-fired (Oliver, 2010). Corporations are also launching massive layoffs. Due to arbitrary choices, financial institutions have instituted unrealistic age requirements for job applicants and have begun mass-firing employees.

• Nigeria is considered a third world country in terms of its poverty rate. There has been a steady rise in the poverty rate. As time goes on, the gap widens between the wealthy and everyone else. Little businesses have been unable to get off the ground due to a lack of essential services and an epileptic electricity grid.

• When it comes to corruption, Nigeria is third on the list of the world's most corrupt countries. Corruption permeated every aspect of Nigerian society up until 1999.

• True e-business is being impeded by a lack of standards, laws, and a computer security and protection legislation, according to Charles Emeruwa, a consultant to the Nigeria Cyber Crime Working Group (NCCWG). The prevalence of outsourcing and foreign direct investment (FDI) is contributing to the problem of computer misuse and abuse.

• To properly monitor and apprehend criminals, cutting-edge information and communication technology equipment are required, which is not already in place due to a lack of infrastructure.

• One reason these horrible crimes have gone unpunished is because there are no comprehensive national databases that could help identify and apprehend those responsible by examining criminal histories and following leads.

• An abundance of cybercafes has sprung up as a result of desperate business people looking for a way to make ends meet. These establishments provide a safe space for syndicates to engage in illicit activities, such as providing night surfing services to potential clients, without interference from authorities.

• The Internet is open and accessible to everyone, because of its porous nature and the lack of a governing body. Consequently, the current form of chaos.

Complexities of Cybercrime

Computer crimes are becoming more difficult to detect and investigate due to the rapid development of modern information technology. An example of this is the widespread availability of global communications networks; nowadays, even a modest personal computer may easily connect to sites on other continents or even hemispheres (Moses-Òkè, 2012). The availability of evidence, investigation coordination, jurisdiction, and the application of current legal frameworks to crimes committed in this environment are all significant concerns.

In addition, brand new concepts with no precedent or legal basis arise alongside emerging technologies. But a virus drains the system's resources without the owner's knowledge or permission. Thus, even a benign virus could be perceived in various ways: as a breach into the system, as cyber-vandalism, or as an annoying practical joke (International Telecommunication Union, n.d.). Keep in mind that the current system for defining and prosecuting computer crimes is reactive and fails to take into consideration any acts or behaviours that may involve innovative computational concepts.

One of the abstract aspects of the information is that it can be copied or stolen and yet stay in the owner's ownership. As it seeks to address computer-related cases, this has perplexed the legal system over the last decade. Copyright, patent rights, and theft as we know them from the physical world plainly do not apply when it comes to software and data stored on computers (Olumide & Victor, 2010). The most obvious reason for this is that when people think of stealing, they usually picture physical harm or irretrievable loss.

Moreover, connected characteristics include the breadth and relative simplicity of digital information's translation and transformation capabilities. What this means is that data, or a code in this example, can be expressed in practically endless ways

(Strassmann, 2009). Mathematical transformations, encryption, and even holographic picture or audio conversion are among the numerous possible formats, in addition to source and executable. If one knows the transformation method(s), one can get the original format back, whether it is audio, pictures, or encrypted text (Olumide & Victor, 2010). With that said, the current state of data may one day be deemed entirely unauthorised (Oliver, 2010). This information's commercial and legal status may instead be dictated by its inherent usefulness or value.

Finally, system breaches can be caused by data changes or alterations, since data can be encrypted or temporarily inaccessible instead of deleted, corrupted, or erased (Schaeffer et al., 2009). Such actions are not properly characterised as theft or even malicious damage.

Combating Cybercrime

To address cybercrime, the following measures can be implemented:

i. Education: Proving cybercrime in Nigeria is challenging due to the absence of a conventional paper audit trail. This necessitates the expertise of computer technology and internet protocol specialists. Therefore, it is crucial to educate citizens about the importance of consistently maintaining and updating the security of their systems when using the internet. It is vital to provide instruction to companies and organisations on the optimal methods for efficient security management. As an illustration, several prominent organisations currently enforce a policy mandating that all systems under their jurisdiction adhere to stringent security protocols. Automated updates are distributed to all computers and servers within the internal network, and every new system must adhere to the security policy before being connected to the network.

ii. Implementation of Programmes and IT Forums for Nigerian Youths: Given that the high rate of unemployment in the country has greatly contributed to the prevalence of e-crime in Nigeria, it is imperative for the government to establish job opportunities for these young individuals and establish IT laboratories/forums where they can

gather and showcase their skills. This may be utilised effectively to promote the growth of the IT industry in Nigeria while also providing substantial rewards for those who introduce innovative ideas.

iii. Address Verification System: The Address Verification System (AVS) can be utilised to verify that the address provided on your purchase form (for customers receiving orders from countries such as the United States) matches the address to which the cardholder's billing statements are sent.

iv. Interactive Voice Response (IVR) Terminals: Interactive Voice Response (IVR) Terminals are a novel technology that purportedly decreases charge backs and fraud by obtaining a "voice stamp" or voice authorization and verification from the consumer prior to the merchant dispatching the order (Olumide & Victor, 2010)

v. IP Address Tracking: It is possible to create software that can track the IP address of orders. This software can be utilised to verify whether the IP address associated with an order matches the country specified in the billing and shipping addresses.

vi. Implementation of Video Surveillance Systems: The challenge associated with this approach lies in the need to carefully consider human rights concerns and legal entitlements.

vii. Antivirus and Anti-spyware Software: Antivirus and anti-spyware software are computer programmes designed to detect, prevent, and remove computer viruses and other harmful software. Anti-spyware programmes are utilised to prevent the installation of backdoor programmes, Trojans, and other forms of spyware on a computer.

viii. Firewalls: A firewall safeguards a computer network against unauthorised intrusion. Network firewalls can exist as either hardware devices, software programmes, or a combination of both. A network firewall serves to protect an internal computer network against unauthorised access originating from outside the network.

ix. **Cryptography:** Cryptography is the field of study that deals with the techniques of encoding and decoding information. Encryption is analogous to the act of sending a physical letter to someone, but with the added security of a lock code on the envelope. This lock code is only known to the sender and the intended receiver (Schaeffer et al., 2009). Several cryptographic techniques have been devised, and a few of them remain unbroken.

x. **Cyber Ethics and Cyber Legislation:** Cyber ethics and cyber legislation rules are being developed to prevent cybercrimes. Each individual has a duty to adhere to cyber ethics and cyber regulations in order to mitigate the rising number of cyber-crimes (Odinma, 2010). It is essential to install security software such as antivirus and antispyware on all computers to ensure protection against cybercrimes. Internet Service Providers should ensure robust security measures at their servers to safeguard clients from viruses and dangerous programmes.

Conclusion and Recommendations

Cybercrimes are likely to increase in frequency as both the general public's familiarity with and proficiency with computers grows, along with the capabilities of the underlying computing technologies. Among the nations with the greatest rates of cybercrime, Nigeria ranks extremely high. When it comes to the country's reputation abroad, cyber security is a major issue that needs immediate attention. An effective first line of defence against cybercriminals should consist of legally binding deterrents and well-thought-out technological solutions specific to the sources of spam (the sending parties). Information attacks can originate from any location and be initiated by anyone. Attackers can evade detection for an extended period of time and evade countermeasures too. Government security agencies should take note: technology and security developments must be kept up with. Professionals in charge of cybersecurity will never win if they lag far behind cybercriminals.

It is imperative to tackle cybercrime from every angle if we are to succeed. The general population, internet service providers (ISPs), cybercafés, the state, security organisations, and internet users themselves must all work together to foster a culture of security awareness. Furthermore, it is critical to address enforcement-related

concerns in depth from a strategic perspective. When enforcement is not done properly, it might have unintended consequences.

References

Adebusuyi, A. (2008). The Internet and Emergence of Yahooboys sub-Culture in Nigeria. International Journal of Cyber-Criminology, 0794-2891, 2(2), 368-381, July-December.

Amaka Eze. (n.d.). Thisday Live.

Anderson, R., et al. (2012). Measuring the cost of cybercrime. 11th Workshop on the Economics of Information Security (June 2012). Retrieved from http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

Background Check International. (n.d.). Information Technology/Cyber Security Solutions.

International Telecommunication Union. (n.d.). Retrieved from http://www.itu.int/en/Pages/default.aspx

Longe, O. B., & Chiemeke, S. (2008). Cyber Crime and Criminality In Nigeria – What Roles Are Internet Access.

Moses-Òkè, R. O. (2012). Cyber Capacity Without Cyber Security: A Case Study Of Nigeria's National Policy For Information Technology (NPFIT). The Journal Of Philosophy, Science & Law, 12, May 30, 2012. Retrieved from www.Miami.Edu/Ethics/Jpsl

Odinma, A. C. (2010). Cybercrime & Cert: Issues & Probable Policies for Nigeria. DBI Presentation, Nov 1-2.

Oliver, E. O. (2010). Being Lecture Delivered at DBI/George Mason University Conference on Cyber Security holding, Department of Information Management Technology Federal University of Technology, Owerri, 1-2 Nov.

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

Schaeffer, B. S., et al. (2009). Cyber Crime And Cyber Security: A White Paper For Franchisors, Licensors, and Others.

Strassmann, P. A. (2009). Cyber Security for the Department Of Defense. Retrieved July 10, 2011, from http://www.strassmann.com/pubs/dod/cybersecurity-draft-v1.pdf