

Analysis of Cybercrimes, Major Cyber Security Attacks and the Overall Economic Impact on Nigeria

Washima Tuleun

Abstract

Cybercrime is a worldwide issue, and Nigeria is not resistant to its impacts. This paper explores the cybercrimes and major cyber-attacks that have targeted businesses and institutions inside Nigeria, looking at different shapes, economic and the financial effect they have on people, businesses, and the country at large.

With the tremendous growth in technological developments coupled with the increased adoption and acceptability of online internet services, there are also been an increase in cyber related attacks and crimes in parallel targeting personal identifiable data, exploitation of vulnerabilities in systems and theft of sensitive data consequently leading to financial loss, reputational damage and overall impact on businesses and institutions.

The study utilizes a comprehensive review of existing writing, case studies, and measurable information to have a holistic understanding of the cybercrime landscape. It moreover examines the measures taken by the government and private sector to combat these violations and proposes recommendations for more successful procedures to mitigate and reduce their affect.

Keywords: Cyber Attacks, Cyber breach, Cybercrime, Cybercriminal, Phishing, Malware, Impact, DDoS, West Africa, Nigeria, Fraud, Threat, Trojan

Date of Submission: 13-06-2024

Date of acceptance: 27-06-2024

I. Introduction

Cybercrime has become a major global pandemic which has grossly been increased by astronomical growth and technological advancements. In Nigeria, the cybercrime has increased due to the growth, adoption and increased integration of digital technologies in the core fibre of daily usage by the populace. The cyber related crimes range from financial fraud, social engineering, identity theft, software piracy, hacking, cyber espionage, and many more [1]. The economic, financial and reputational implication and potential impact of cybercrime related activities are significant, with potential negative ramifications on the national economy, business operations, and personal security [2].

The increased adoption of digital technologies has fundamentally transformed Nigeria's socio-economic landscape, overall driving innovation, improving connectivity, and stimulating strong economic growth [3]. However, it is important noting that with the rise in digital evolution also comes with accompanying cybersecurity challenges, with cybercrime emerging as a significant and growing threat due to the widespread network of interconnected devices in the digital realm [4].

Several sectors are affected however the financial institutions, in particular, over the years are

increasingly becoming prime targets, due to the level of sophisticated attacks that exploit vulnerabilities in online banking systems. In addition cybercriminals are devising new methods such as the adoption of cryptocurrency to receive payment, launder proceeds of crime and ultimately evade detection in the process [5].

The of impact of cybercrime from an economic perspective is significant, whilst financial losses from cyber related attacks is mostly classified as among the top segments businesses are mostly affected, indirect loss such as damage to business reputation and break down of customer trust, financial investment lost are some of the impacts of cyber-attacks, breaches and crimes which further exacerbate the economic burden [6]. Moreover, the substantial investments required for cybersecurity measures, including technology upgrades, personnel training, and compliance with regulatory standards, place additional financial strain on organizations.

In response to the increase in cyber related crimes within Nigeria and the overall impact to the Nigerian economy as a whole, the Nigerian government have developed and implemented policies and act with the aim of addressing the negative tide. Some of which include the Cybercrime Act 2015, approvals for the establishment of cybersecurity institutions and agencies and also driving to attract skills and private

partnerships with the Nigerian government. Whilst these strategies adopted have shown the initial drive to address the cybercrime issues, there is the need for continuous and intensive adaptation of cybersecurity strategies due to the ever evolving sophistication of the threat actors and cyber threats.

II. Literature Review: Cybercrime Trends

There are various types of cybercrime that are prevalent within Nigeria which is also ranked as a leading country within the African continent as potentially a target of malicious activities, victim and in some instances originator [7]. Cybercrime is often associated with the basic scam attacks however there has been a rise in sophistication of attack types which shows a rapidly changing ecosystem and flagging the African region as an untapped resource for carrying out malicious attacks for illegitimate gains [8].

The rationale for carrying out such attacks range by malicious attacks for a variety of reasons and this is based on the type of threat actor which could be for financial gains, hacktivism, disgruntled employees which can be classed as insider threat actors, nation state threat actors, script kiddies carry out attacks for the thrill and fun among others.

A review has shown that the success of cybercrime activities can be attributed to many factors such as lack of preparedness of institutions, poor patch management process against vulnerabilities, and lack of requisite cybersecurity skill set to detect, prevent and respond to sophisticated threat actors [4].

Due to the growing sophistication of cyber related crimes, institutions and the government is struggling to keep abreast of the ever changes tactics and techniques of threat actors hence the need to understand the scope of the attacks, tactics deployed and potentially the trends which will become an initial starting point in addressing the scourge within the nation at large.

By understanding the complexities and ramifications of cybercrime, stakeholders can develop more robust and proactive approaches to safeguard Nigeria's digital economy.

III. Types of Cybercrime in Nigeria that are prevalent are as follows:

1. Phishing

According to NIST, “*phishing is a technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person.*” [64]

During phishing attacks, the threat actors employed the use of social engineering by luring unsuspecting users to malicious websites with the sole aim of stealing user credentials and sensitive details used to carry out unauthorized and malicious activities. Phishing have been classed as one of the most common form of security breach as highlighted by the official statistics from the cybersecurity breaches survey 2020 in the United Kingdom. [9]

Other phishing attacks are not focused on just stealing credentials but have the objective of tricking users to click on malicious embedded link with an email which will potentially download malicious attachments and payload infecting the system with more dangerous malware such as Ransomware.

Phishing attacks are successful based on a number of factors such as poor security habits of users, lack of security training around phishing detections, usage of default passwords, and lack of the usage of multi factor authentication among others.

1.1 How does phishing attack work?

Phishing occurs following 4 phases which are highlighted below:

- **Phase 1:** This is the phase in which the attack sends a carefully crafted email to the potential victim with the aim of getting them to click on malicious embedded emails and input their credentials which will be stolen
- **Phase 2:** The aim of the second phase is to get the potential victim to click on the malicious link and visit the fake website however designed to look real and authentic.
- **Phase 3:** This phase requires the victim to enter their credentials which will be retrieved by the malicious actor

- **Phase 4:** The malicious actor now has access to the victim credentials and uses it to carry out nefarious activities.

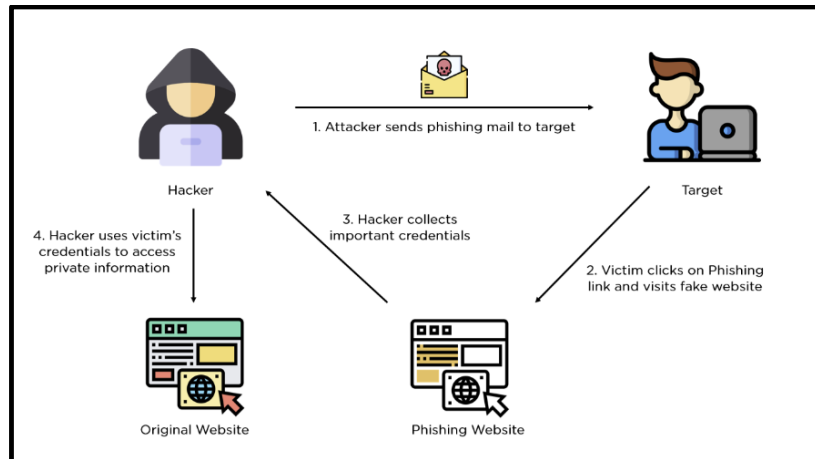


Fig. 1 – Process flow of a phishing attack
 Source: Simplilearn [10]

1.2 Types of phishing attacks and Techniques

a. Standard Email Phishing:

The threat actor carries out a mass campaign targeting an organization with the hope of getting lucky with someone clicking on the malicious

embedded link within the email potentially asking the end user to enter their user name and password to access a link, URL or website portal. In some cases, these mass email campaigns are designed poorly with grammatical error or expressing a sense of urgency to have a task completed.

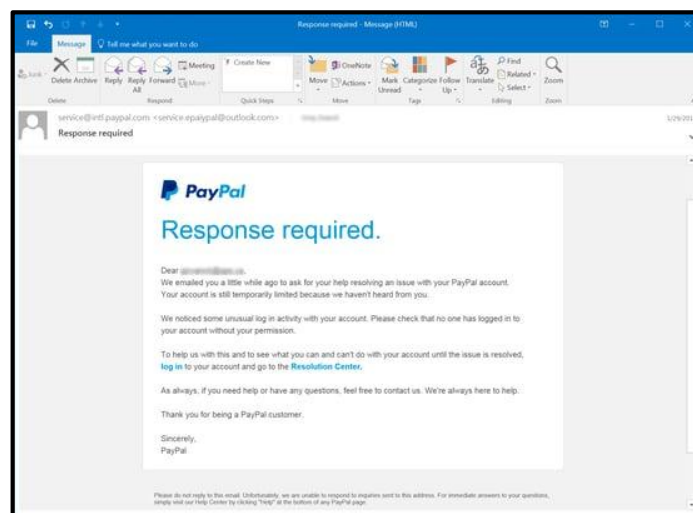


Fig. 2 – Standard Phishing Email Example
 Source: knowbe4 [11]

b. Spear Phishing

With spear phishing, the attack is targeted and premeditated in the sense information about the victim is harvested potentially via open source techniques. The threat actors normally present themselves as genuine persons and business contact and tend to craft the email in a personalised format which tend to have specific details with the aim of getting the trust of the potential victim as the case may be. [12]

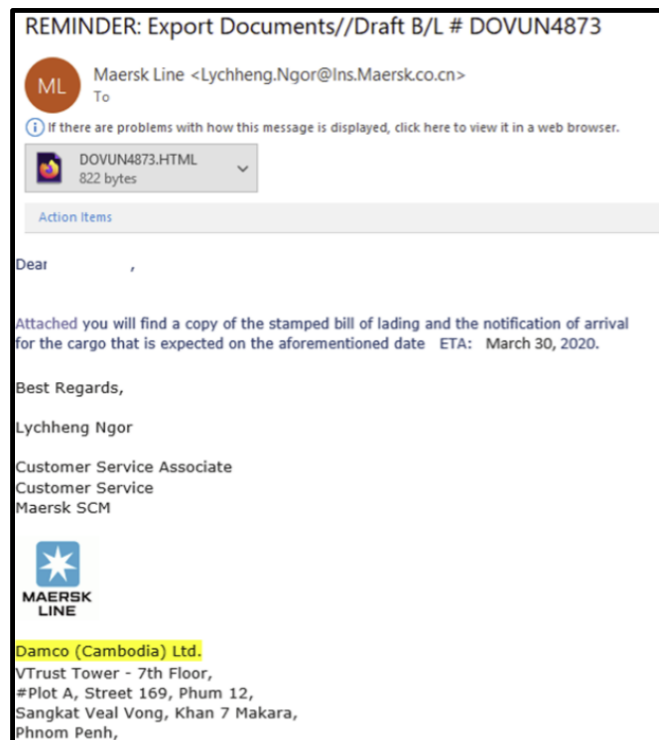


Fig. 3 - Example of a Spear Phishing Email
 Source: Cheapsslsecurity [13]

Spear phishing emails can often be difficult to spot. This is largely due to the extensive effort put in by the attacker to make the spam seem as authentic as possible.



Fig. 4 – How Spear Phishing Works
 Source: InfosecTrain [14]

c. Whaling

This is a type of phishing attack aimed at the senior level executive such as the “C-Level” e.g. COO, CMO, CEO, CISO. This involves high level of sophistication targeted at getting the executive to part with huge some of funds to the malicious actor.

An extensive amount of research is done by the hacker to decide on the manner and the appropriate time for these attacks.

Sophistication of the attack could include the creation of a specifically crafted domain name similar to the recipient email domain. This is known as a typo squatted domain which means the attack

legitimately registers a domain more closely with that of the recipient domain with the aim of deceiving the potential victim and making it seem legitimate.

In some instances, there are no attachments embedded to the whale email or URL link within the email. This makes it easy to bypass potential email securities such as email security policies, AV engine or sandbox solutions which makes the email appear legitimate to the recipient.

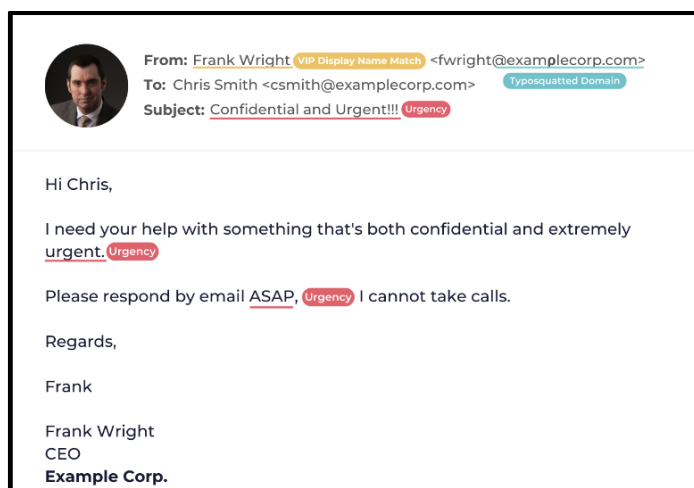


Fig. 5 - Example of a Whaling Phishing Email:
Source: meshsecurity [15]

d. Pharming

Pharming is an attack similar to that of phishing however in this instance there is a redirection of the website traffic to that desired by the threat actor via manipulation of actual URL and ultimately confidential information is stolen. This is possible via the installation of malicious code on the victims system of interest to the attacker.

In summary, it is the act of potentially spoofing or creating a fake website and redirect users away from legitimate websites to the malicious domains.

The objective of pharming attack is also to capture the victim's credentials, username, password and personal identifiable information.

The steps carried out by the threat actor as follows:

- **Step 1:** The threat actor sets up a malicious website which is designed to look like that which is legitimate which is the used primarily for the

collection of sensitive data that are entered potentially by the victim

- **Step 2:** The attacker changes or modifies the domain name service (DNS) entries within the host file of the victim's endpoint. This ensures redirection to the malicious URL of interest once the victim attempts going to the original legitimate website. This is regarded as DNS cache poisoning.

- **Step 3:** This step requires the victim to input their credentials such as username, password, credit card data and sensitive data or have the victim interact with the malicious URL redirect.

- **Step 4:** This is the last step which involves the threat actor collection of the sensitive data entered by the victim which potentially results to data theft, financial fraud or gain unauthorized access to the victim's account.

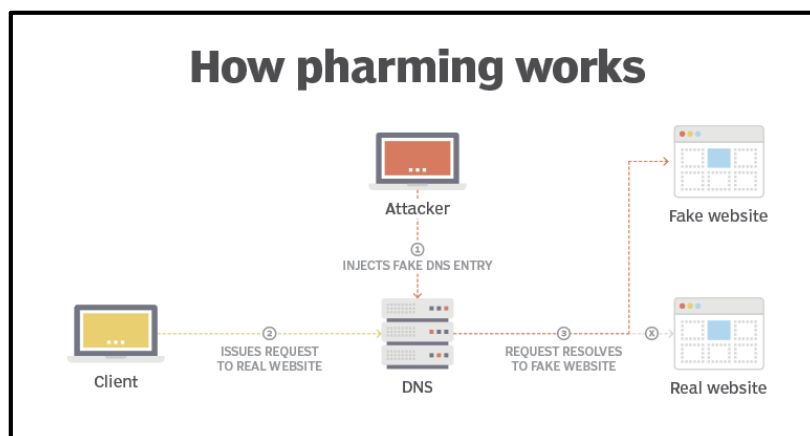


Fig. 6 – How Pharming works
 Source: techtarget [16]

e. Smishing

This attack type makes use of fake text messages sent to the victim’s mobile device which is aimed at getting the users to click and download malicious applications and also share sensitive data.

The increase of bring your own device (BYOD) and remote work arrangements have also led to more people using their mobile devices at work, making it easier for cybercriminals to access company networks through employees’ cell phones.

It is quite difficult spotting malicious links on mobile devices in comparison to laptop devices where once can easily hover on the embedded link to ascertain its legitimacy. The steps carried out by the threat actor as follows:

- **Step 1:** The malicious threat actor crafts and sends out the text message designed to alarm, intrigue or entice the recipient.

For example it could be a message saying “you have been selected among the 10 lucky winners for a trip to Dubai” or a message stating “suspicious activities have been observed on your bank account and you need to respond fast”, all this with the aim of getting the recipient to take immediate action.

- **Step 2:** This is a combination of multiple actions such as

- a. Disguising the sender ID of the message or having this spoofed to make it look like coming from a trusted source like your University or Bank.
- b. Including a call to action, which might be to have the user call back, click on the link in the message, reply to the message with certain details or install an application for support purposes
- c. Victim responds or falls for the bait and potentially give access to their sensitive data.

- **Step 3:** Data theft by the malicious attacker which can then be used for carrying out identity theft, fraud or gaining unauthorized access to the victims account.

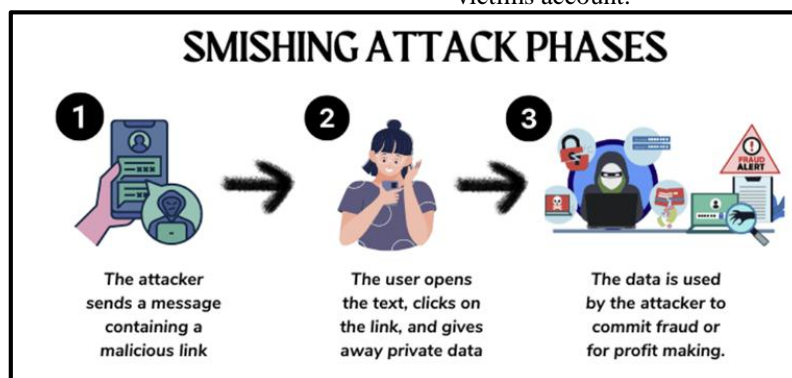


Fig. 7 – Smishing Attack Phases
 Source: heimdalsecurity [17]

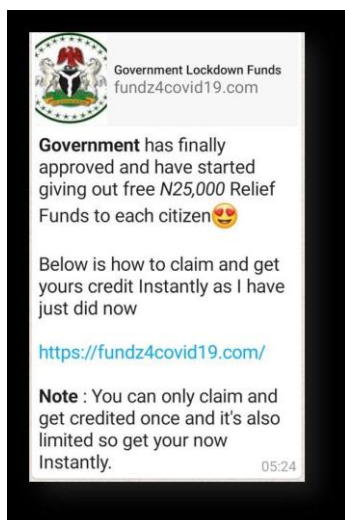


Fig. 8 - Sample Smishing messages

Source: [18]

f. Vishing

This term is formed by blending 'voice' and 'phishing', is a type of phishing attack that involves phone calls or voicemail messages.

The attackers tend to utilise persuasive tactics and social engineering to get the victim to share sensitive data and credentials over the phone purportedly from a legitimate institution.

The threat actor tends to assume the role of a representative of an institution such as financial services or other institution with the objective of getting the user to release their personal identifiable information or credentials. [19]

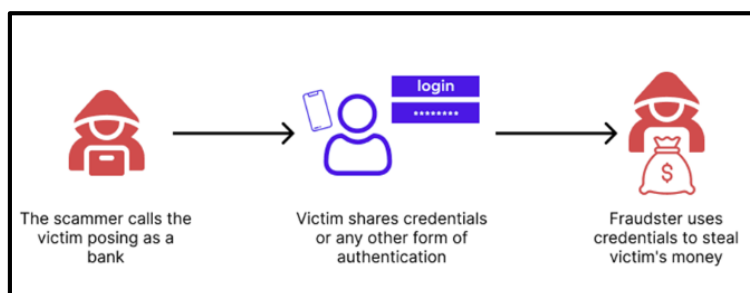


Fig. 9 – How Vishing works
 Source: (Clearvpn, 2024) [20]

The attacker makes the phone call, if the target answers, the attacker will impersonate a representative from the trusted entity they're pretending to be, creating a sense of urgency that prompts the victim to share their sensitive information. If the call goes to voicemail, the attacker will typically leave an automated message. This message will ask the target to call back a specific number - a number also controlled by the criminals. [20]

If the victim returns the call or stays on the line, they're prompted by the criminals (or their automated system) to enter their private information. This could be bank account numbers, credit card details, passwords, or even their social security number which leads to compromise of the victim's sensitive data and information.

2. Malware Attacks

According to "Bossler, A.M., Holt, T.J., 2009. *Online activities, guardianship, and malware infection: An examination of routine activities theory. International Journal of Cyber Criminology*. 3 (1), 400-420.", [21].

Malware is an abbreviated form for malicious software which is used and ultimately designed for exploitation, cause harm and potentially compromise a system or network.

2.1 Types of Malware

- **Viruses.** This is a type of malware that requires a user action to spread just like opening an infected file. It basically corrupts or modifies files of interest and potentially spreads and replicates itself via multiple methods for example opening of email attachments, downloads or removable media.

Viruses have unique characteristics ranging replication of itself and spreading across the business estate when certain criteria are met such as erroneously clicking on a malicious embedded links in emails or remaining dormant pending meeting other trigger mechanisms.

It is important to note that viruses tend to carry payloads capable to causing harm to computer networks, aiding in the theft of credentials or destructive mechanisms such as deletion of files and data.

There are various types of viruses some of which include macro virus, polymorphic virus, boot sector virus and file infector virus. Viruses spread via many methods such as email attachments, Removable media, network shares etc.

- **Worms.** This is a type of virus that is stand-alone and does not require human interaction to replicate itself across computers and causes damage and disruption.

Characteristic of worms include the following: They are stand-alone hence do not require hosts to operate or attach themselves to host files or programs, significant network consumption of resources, the primary method of propagation is via network connections and exploitation.

Some types of worms include email worms, internet worms and file sharing worms. Some popular worms include WannaCry worm, Morris worm, and code red worm among many others.

- **Trojans.** This is a type of malware that is disguised as a legitimate program to try and gain unauthorized access to the victim's system. They typically get hidden as an attachment in emails or free to download files with the ultimate aim of getting downloaded onto the victim's system [22].

A Trojan virus spreads through legitimate-looking emails and files attached to emails, which are spammed to reach the inboxes of as many people as possible. When the email is opened and the malicious attachment is downloaded, the Trojan server will install and automatically run every time the infected device is turned on. [23]

Trojan horse does not attempt to inject itself into files however focuses more on the theft of sensitive information from the victim's computer and asset. Some further characteristics of Trojan include appearing as legitimate or benign applications with the ultimate aim of deceiving the end user to download the application, Trojans are non-self-replicating and rely on social engineering to be installed on systems and potentially create back doors to gain and maintain remote access.

Classification of Trojans include the following

- a. **Remote access Trojans** which provides threat actors with complete control once the system or network has been compromised allowing them to manipulate the files, processes and execute commands.

- b. **Spyware Trojans** which are Trojans focused on the theft of user activities, key logging activities and also capturing screenshots of victims systems with the objective of stealing sensitive data and credentials.

- c. **Ransomware Trojans** which aim to encrypt victim network and systems with the objective of getting ransom payments in exchange for the decryption keys.

- d. **Banking Trojans** are focused towards the financial sector with the aim via phishing email attacks for stealing sensitive financial information such as credentials, credit card details etc.

- e. **Backdoor Trojans** creates backdoor on the victim's system to gain remote access and control which could be used for data theft and executing other commands.

Examples of popular Trojans include Emotet, Mirai, agent tesla, Zeus Trojan among many others.

- **Ransomware.** *A threat that is increasing gradually for the last couple of years. Usually, it encrypts users' files or steal/delete important information and holds the decryption key until a ransom is paid by the victim* [24]

This form of cyber extortion has become increasingly prevalent, affecting individuals, businesses, and governments worldwide. It is always important to ascertain how the malicious attacks gained entry into the network to ensure once remediated do not gain access again into the system.

Ransomware ensures the encryption of files on the system rendering them unusable and following up to demand for Ransomware to have access to the decryption keys to have the files unencrypted. They typically demand for payment to be made in cryptocurrency and this is done by displaying the ransom note on the affected system's screen. [25]

In some instances, the threat actors also include a deadline to have payments made after which the commence the deletion of the victim's files that they have encrypted initially leading to total loss of data, unless in instances the company has a structured backup process in place to restore from in such scenarios.

There are different types of Ransomware ranging from crypto Ransomware for example WannaCry,

locker Ransomware, scareware which displays fake malware and virus warnings and request for payments, leakware which threatens to publish stolen data unless payment is made to have them retrieved, just to name a few.

Ransomware can be transmitted via multiple methods ranging from phishing emails attacks which can act as initial entry points by containing malicious attachments or embedded links within the email which when opened or clicked acts as the initial entry point for Ransomware.

Other methods include the exploitation of vulnerable websites, software or operating systems. For instance, threat actors could carry out scanning and exploitation of outdated or unpatched software to gain access into systems. Via Removable devices and also social engineering which involves psychological manipulation to trick users into performing actions that lead to Ransomware infection.

- **Spyware.** This involves stealing sensitive data without the victim's consent and sending the data to malicious actors using unwanted software that monitors the system. Attackers use different types of spyware to infect users' computers and devices. Each spyware variant collects data for the attacker, while less serious types of spyware monitor and send data to third parties such as advertisers, data collection companies, and malicious actors. [26]

The most common types of spyware include the followings.

- a. **Adware.** Focuses on monitoring users, compromising users' privacy, end devices and the potential sale to advertising units. They also end up serving and delivering automatically various malicious advertisements in intrusive manner to the end users. This are often in the form of pop ups banners or browser advertisements.

Adware tends to consume quite a bit of system resources which can affect the performance of the system leading to degraded performance and poor user experience. They also tend to be bundled into other legitimate software which makes it difficult to detect and unsuspecting by the end users, embedded into malicious website pages or phishing emails. The main goal of adware is to make money for the people who create it. Income is commonly generated by pay-per-click schemes, affiliate marketing, or the sale of gathered user data.

- b. **Rootkits.** They are malicious applications designed to be stealth and low level within the system with the aim of avoiding detections and difficult to remove. They are designed to gain unauthorized access, maintain persistence, and carry out privilege escalations via the exploitation of vulnerabilities.

There are various types of rootkits ranging from kernel mode rootkits, user mode rootkits, boot kits, firmware among many others.

- c. **Keyloggers** are a type of info stealers installed on the target's system designed for logging and recording users every key strokes made on compromised systems with the aim of collecting sensitive information entered by the victim such as passwords, credentials, credit card information, email data, passwords, text messages etc. They could be hardware Keyloggers, software Keyloggers or firmware Keyloggers.

3. Denial/Distributed of Service Attacks

Denial of service attacks focuses on affecting the availability of systems, applications and network. The attack tends to focus on targeting the system resources and pushing it to its limits to have it run out and affecting the availability of the systems by overwhelming the infrastructure such as bandwidth, memory, CPU power, or disk space, making it incapable of handling legitimate requests with a flood of illegitimate internet requests or traffic. [27]

DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices [28]. The attack is carried out via a web of interconnected systems which are potentially compromised and infected by malware and remotely controlled by the malicious threat actors. They are referred to as bots or botnet. The attackers tend to use the botnet to target the infrastructure of interest with the aim of overwhelming the resources since it is difficult to differentiate the legitimate traffic from illegitimate traffic.

DDoS attacks happen for a variety of reasons ranging from the financial gains by the malicious actors demanding for ransom payments, hacktivism efforts to show their support for a particular cause or competition among threat actors

There are various types of DDoS attacks including:

a. **Application layer attack** which is aimed at overwhelming the target resources. Example include HTTP flood attacks. This assault is like repeatedly hitting the refresh button on numerous

computers simultaneously, overwhelming the server with a high volume of HTTP requests and causing a denial-of-service.

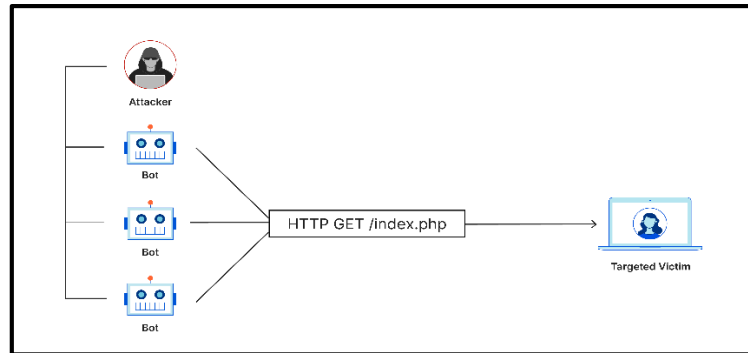


Fig. 11 – Application Layer Attack
 Source: CloudFlare [29]

b. **Volumetric Attacks** which aimed to affect the availability of the system by flooding it with large amount of traffic either through amplification or requests from botnets with the aim of causing it to slow down or ultimately fail. Examples include the ICMP flood and UDP flood attacks. This type of attack causes congestion between the targeted infrastructure and the larger internet.

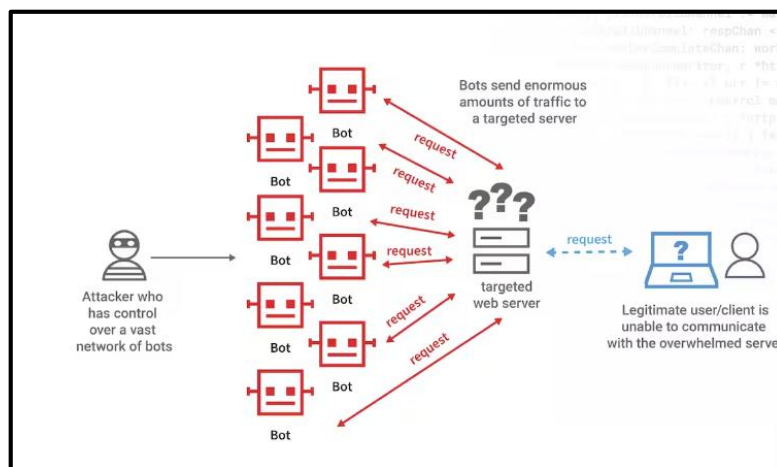


Fig. 12 - Volumetric Attacks
 Source: Akamai [29]

The server, network device, or security defenses struggle to differentiate between legitimate and malicious traffic due to the large volume of users. As the server attempts to handle and address every request in the incoming traffic, available resources like bandwidth, processing power, and memory are used up. [29]

There are several types of volumetric attacks ranging from ICMP flood attacks, DNS reflection attacks, UDP floods, TCP out-of-state floods, reflection amplification attacks

c. **Protocol attacks** targets network and transport layer of the OSI model to render the target unavailable. This is done by over consuming the target resources with excessive requests by exploitation of the TCP handshake process and sequence which is done by sending excessive amounts of initial connection SYN packet requests with spoofed IP addresses forcing the target to respond to each one waiting back for a response which never happens there by exhausting the target resources.

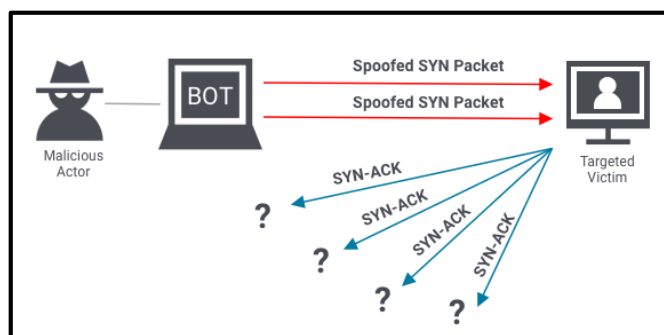


Fig. 13 - Protocol attacks
 Source: Onelogin [30]

4. Insider Threats

Insider threat refers to threats originating from within an organisation or institution based on the fact the insider has information about the inner works of the institution, ranging from policies, process and best practices. This makes attacks carried out to have massive impact based on this fact which could be intentional or un-intentional. [31]

The insider threat actors could be malicious intentional threat actors or negligent unintentional threat actors. Detecting insider threat actors can be very difficult due to the level of trust already established by the actors since they are already in the organisation, understanding of the infrastructure and processes within the company and institution and difficulty in identifying behavioural patterns of the actors. [31]

A “2020 Global Cost insider threat” report by proofpoint, showed that 60 percent of companies experienced an average of more than 30 incidents per year and the overall cost of insider threats is rising, with a 31% increase from \$8.76 million in 2018 (Ponemon) to \$11.45 million in 2020. [32]

5. Financial Fraud

Financial fraud is one of the most common forms of cybercrime in Nigeria. This includes phishing scams, online banking fraud, and credit card fraud. Cybercriminals often exploit weaknesses in online banking systems to steal money or sensitive information.

According to FATOKI, JACOB, 2023, cyber fraud is the use of social engineering and deception strategies which is aimed at deceiving others for the purpose of financial gain, theft of money and having potential negative outcomes on the victims. [33]

This could be via phishing emails, persuasive phone calls or text messages aimed at duping someone to disclose sensitive information or secrets. There are various forms of financial frauds or attacks ranging from online scams, phishing attacks, skimming of card data without the victim’s knowledge and identity theft during legitimate transactions which involves the unauthorized acquisition of personal information, which is then used to commit fraud. In Nigeria, this often manifests in the form of SIM swap fraud, where criminals take control of a victim’s phone number to access banking information.

IV. Methodology

The methodology adopted is based on assessment of secondary data sources such as research papers, government policies, publication journals newspaper and the internet. The study is descriptive in nature based on existing works about cybersecurity trends and attacks globally and within Nigeria

V. Case Studies and Recent Attacks

a. Case Study 1: MTN’s mobile money - MoMo Payment Service Bank Hack

In 2022, MTN subsidiary payment service MoMo experienced a potential breach reportedly in the tune of \$53 million as a result of unauthorized transactions and transfers to approximately 8,000 accounts with Nigerian banks. [34]

Whilst MTN claimed to have worked to have the issue remediation and further transactions stopped. A statement was released as per the screen shot below and MTN is suing the 18 banks requesting for a refund of the remaining unauthorized monies transferred in a suit marked FHC/L/CS/960/2022 and filed on May 30, 2022 and also to make available information relating to the transactions

such as account names, destination accounts and banks to aid in tracing and recovery of the funds. [35]

However, no evidence was shared with regards detailed events of how the incident occurred with regards potential initial entry points, if existed among, other details. The Nigeria Data Protection

Commission (NDPC) is currently conducting investigations into the alleged data privacy breach which could potentially lead to penalties if found wanting. [36]

The institution released an official statement confirming the statement as per the below:



Fig. 14 – Momo official statement confirming
Source: MoMo, 2022 [37]

b. Case study 2: Patricia, a leading Nigerian Crypto Marketplace, suffers Breach

In 2022, Patricia, a leading Nigerian Crypto marketplace experienced a severe security breach that compromised its financial assets resulting in potentially loss of customer finance with Bitcoin and Naira assets affected since the Patricia Personal arm of the business was affected which is the retail trading application. [38]

The institution released an official statement confirming the statement as per the below:



Fig. 15 – Patricia Official Statement
 Source: Downtime Update [39]

c. Case study 3: Babcock University Website Hack

On the 23rd March 2023, Babcock University website was compromised and explicit adult content posted with the intent of potentially embarrassing the institution. According to statements published, the threat actors threatened repercussions based on the records they were able to access as a result of the compromise. [40] The university released an official statement as per the below:

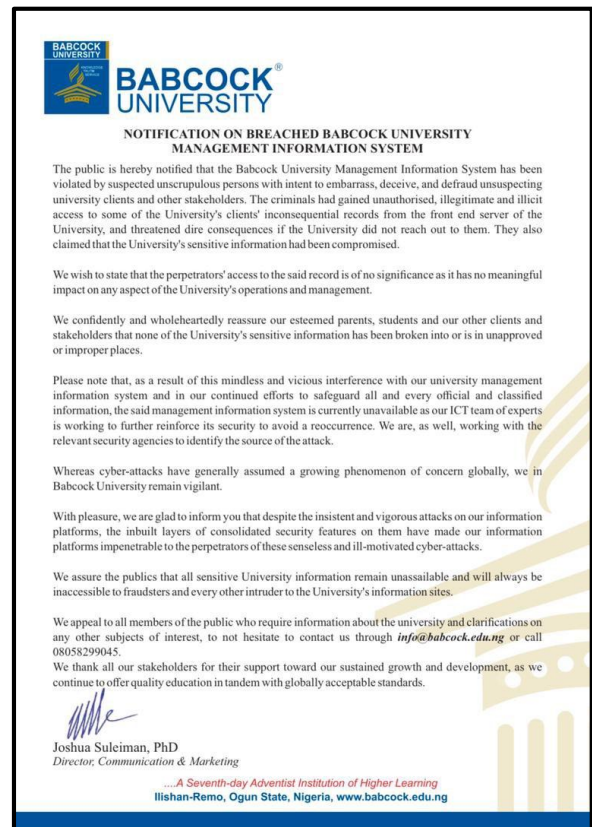


Fig. 16 – Babcock Official Statement
 Source: Babcock, 2023 [40]

d. Case study 4: FUTA Official Website Hacked

In 2016, Federal University of Technology Akure website was compromised. There are no details as to the actions taken or official comments from the institution. [41]

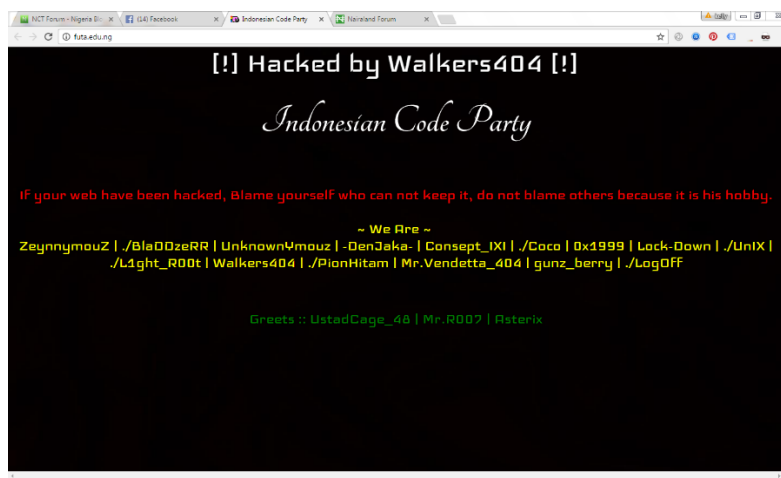


Fig. 17 – FUTA Hacked Website
 Source: Nairaland, 2016 [42]

e. Case study 5: INEC Official Website Hacked

In 2015, The Independent National Electoral Commission (INEC) in Nigeria was compromised in the early hours before the start of the voters' accreditation process. [43]



Fig. 18 – INEC Hacked Website
Source: Channels, 2015 [43]

The institution confirmed the incident as per the below image

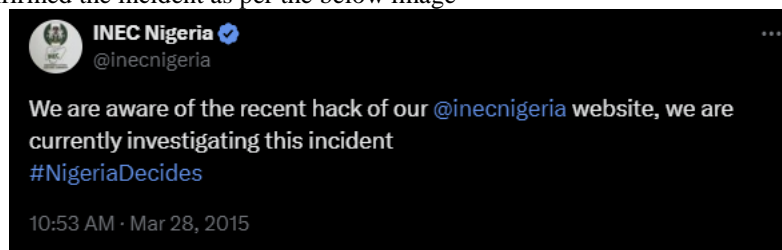


Fig.19 – INEC official statement
Source: INEC Nigeria Update [44]

f. Case study 5: University of Nigeria Nsukka Website Hacked

The official website of the University of Nigeria, Nsukka (UNN) was hacked and defaced in October 2019, by a suspected French hacker identified as Nasty. [45]

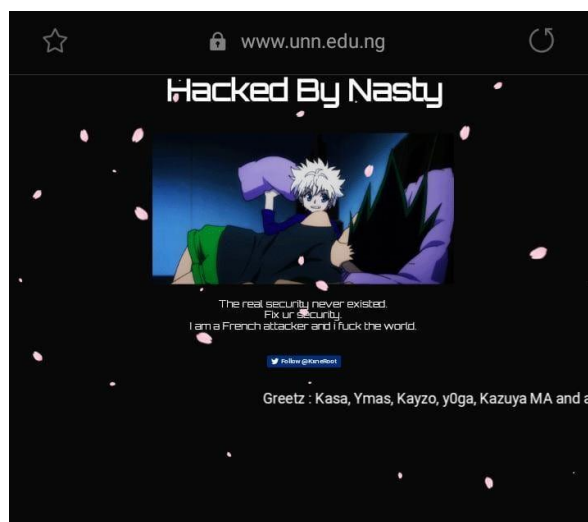


Fig. 20 – UNN Hacked Website Page
Source: lindaikajisblog, 2019 [45]

g. Case study 6: Union bank Fraud

In 2020, Over N2.55 Billion was stolen from Union bank Nigeria via potential connivance to gain access to the banks flexicube database. The monies was subsequently transferred into series of accounts for ease of extraction. The Economic and Financial Crimes Commission (EFCC) has secured the conviction of the culprits. [46]

h. Case study 7: Arik Air grounded by Amazon S3 leak

In October 2018, an unsecure S3 Amazon bucket was discovered to be publicly available containing sensitive personal Identifiable information PII data such as credit cards, email addresses, customer names etc. [47]

An Amazon Simple Storage Service (Amazon S3) bucket is a public cloud storage resource similar to file folders. It stores objects consisting of data and descriptive metadata. [48]

The accessible data could potentially be used for Identity theft, well-crafted phishing email campaign which could potentially lead to large financial loss. Arik Air released official statement below:

Update 11.01 GMT: An Arik Air spokesperson told ZDNet:

"Our attention has been drawn to a reported exposure/vulnerability of customer data on Amazon S3 bucket. We can confirm that we do not use Amazon S3 for our hosting services. Our online platforms are up and running and not under attack. Arik Air takes IT security and protection of customer data seriously. We are reviewing all our systems including interface[s] with third-party processors to eliminate vulnerabilities. We would like to assure our customers of the safety of our online sales platforms."

Fig. 21 – Arik Official Statement
Source: ZDNET, 2018 [49]



- Customer email address
- Customer name
- Customer's IP at time of purchase
- A hash of the customer's credit card
- What appears to be last 4 digits of the credit card used.
- What appears to be maybe be the first 6 digits of the credit card used.
- A unique device fingerprint (presumably the user's mobile or desktop device?)
- Type of currency used
- Payment card type
- Business name related to the purchase (more on this below)
- Amount of purchase
- Date of purchase
- Country of origin of the purchaser


Fig. 22 – Sample copy of details exposed
Source: TheCable, 2018 [48]

i. Case study 8: Surebet247 suffers data breach

In 2020, Surebet247 a sport betting company was a victim of a security incident which potentially puts thousands of customer data at risk which was subsequently reported to the company.

Dumps surebet247.com and more

 To  Sun 29/12

[https://\[redacted\]](https://[redacted])
password zip: 

enjoy

Sent with [ProtonMail](#) Secure Email.

Fig. 23 – Surebet247 file dump
Source: TroyHunt, 2020 [50]

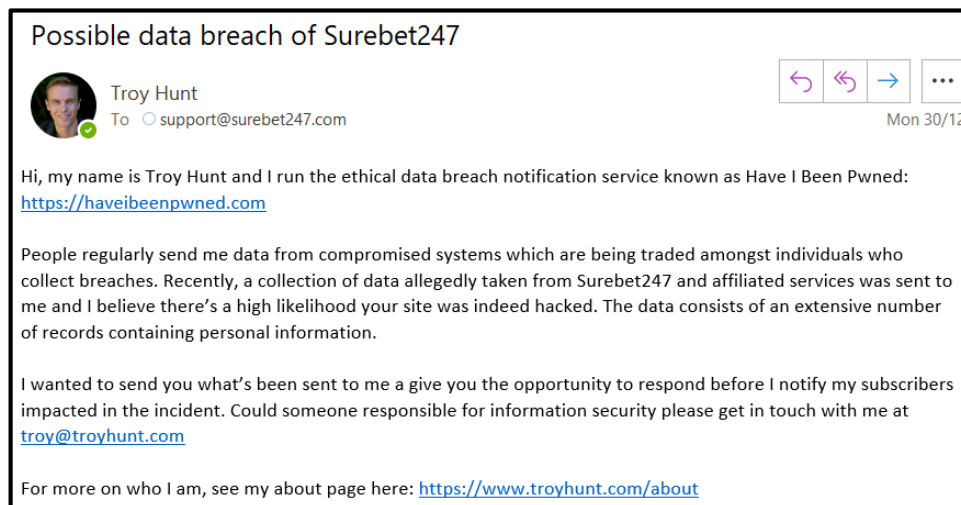


Fig. 24 – Email evidence showing Surebet247 was compromised

Source: TroyHunt, 2020 [50]

j. Case study 9: Jamb website compromise

In April 2021, Nigeria’s Joint Admissions and Matriculation Board (JAMB) has reported that hackers breached its website. The institution released a statement revealing there was a financial loss as a result of the compromise which involved altering the profiles of company staff. [51]

k. Case study 10: The Nigerian government NDDC website was compromised

In 2011, The Niger Delta Development Commission (NDDC) website was compromised by a group of hacktivist in protest to the amount budgeted for the presidential inauguration of the president elect Goodluck Jonathan

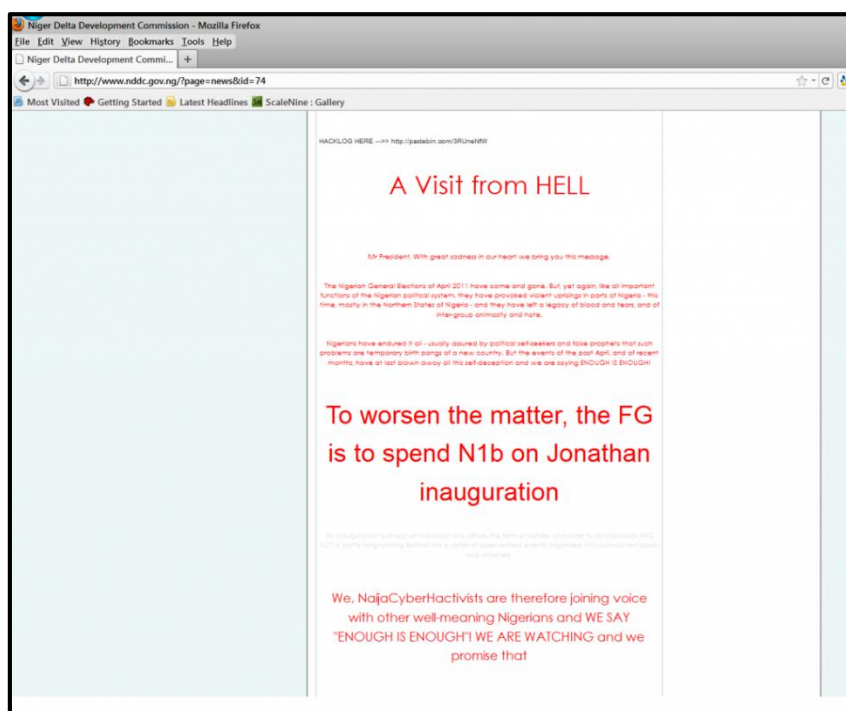


Fig.25 – NDDC Compromise Website

Source: Technext24, 2021 [51]

I. Case study 11: Bet9ja's website hacked by Russian Blackcat group

In 2022, Bet9ja revealed they have been compromised by blackcat group which is a Russian threat actor group and demanding payment of ransom [52]

In an article published on Tripwire and written by Graham Cluley (a computer security expert and writer), BlackCat (also known as ALPHV) is a

relatively new Ransomware-as-a-service (RaaS) operation, which has been aggressively recruiting affiliates from other Ransomware groups and targeting companies globally. [53]

"The Alphv group claimed to have encrypted files on the victims' computers, rendering them inaccessible until a ransom is paid. Bet9ja assured its customers that all funds are safe and the issue will be resolved." [54]



Fig.26 – bet9ja Official Statement
Source: Nairaland, 2019 [55]

VI. Causes of Cybercrime

The primary causes of cybercrime are as follows:

a. **Financial benefits and gain.** This is a primary cause of cybercrime and this is due to the financial benefits that are gotten. This could be via financial fraud in intuitions or demanding for ransom payment as a result of Ransomware before the release of decryption keys. According to Sophos "state of Ransomware 2024" survey report institutions reported an increase in Ransomware payment on an average of \$2 million in 2023 which further goes to show how lucrative this is for malicious threat actors.

b. **Lack of cybersecurity awareness.** This is also a factor based on the fact users and members of staff are not fully aware of the implications and effects of cybercrimes on their institutions. This might partly be due to low levels of security awareness and what they need to do to protect themselves and business against cyber-attacks. This could potentially lead to users clicking on phishing links with emails which would lead to a breach of credentials and the company's network.

c. **Technological advancements.** With technological advancements also brings about weaknesses and vulnerabilities identified within the software and hardware solutions which potentially brings about exploitation of the vulnerabilities by

threat actors for various reasons. There are instances where by security misconfigurations, inadequate or default configuration settings makes it an easy target and interesting for threat actors and attackers.

d. **Anonymity of the internet.** The idea of been anonymous on the internet gives threat actors the courage and motivation to carry out malicious cybercrime activities or conduct illegal transactions without the fear of been caught. This could be via the creation of aliases, routing traffic via VPN services to anonymise IP addresses and traffic among other methods.

e. **Political and Ideological Motives.** Some cybercriminals are driven by various beliefs to carry out malicious activities be it politically motivated which was observed during the invasion of Ukraine by Russia during which we observed a spike in cyber related security incidents for and against the warring parties. Other beliefs could be religious or against government policies as the case may be.

f. **Lack of cybercrime legislation.** Due to the absence of international cyber laws and cross collaboration between countries, cybercriminals know there are no consequences and can easily attack targets or institution from different countries without repercussions.

g. **Economic Disparities.** Poverty, unemployment and economic disparities can be a factor pushing cybercriminals into the life of security related malicious activities either for financial gains, quick profits, survival etc. as the case may be.

h. **Proliferation of Cybercrime tools.** The availability of already packaged tools which does not require in-depth knowledge of security process makes it easy for script kiddies or criminals with limited knowledge be able to carry out cyber-attacks easily. For example Phish as a service solution makes it easy to craft phishing campaigns based off existing templates to target institutions.

i. **Corporate Espionage.** Theft of sensitive data and company intellectual property is also a motivation for threat actors and cybercriminals with the ultimate aim of having competitive advantage over an institution, company or nation state.

j. **Revenge or personal motivation.** This is also a factor since disgruntled former employees can target companies for revenge reasons, if for example they were relieved or sacked from their positions. There are some instances you can have

cybercriminals targeting ex-partners via various methods such as phishing attacks, denial of service attacks or making use of privilege information to negatively impact the target of interest from a negative perspective.

VII. Economic impact of cybercrime

According to “Hassan A. B. et al (2012) [56], some of the identified effects of cybercrime to include reduced competitive edge over competitors or other organizations, poor and potential slow financial growth as well as reputational damage on a national level for the country involved. Other impact of cybercrime as follows:

a. **Financial losses.** Direct financial loss to the company as a result of funds stolen which includes cost of remediation and restoration after a cyber-related incident or crime. There is also the reputational damage since clients and customers have lost confidence and trust which significantly affects profitability and reduced productivity which can also lead further financial loss. According to “Sophos – The state of Ransomware 2024”, the mean cost to recover from a Ransomware attack is \$2.73 million.

b. **Reputational Damage and impact on Investments.** There is reputational damage to the country and geolocation based on the number of cybersecurity incidents attributed to the company or country since it could be classified as high risk by businesses and investors which potentially leads to reduced investments as a result and overall impact on the nation’s macroeconomic stability.

c. **Competitive Edge lost.** A company can lose its competitive edge particularly if they are in a niche and specialised area as a result of theft of their intellectual property which could lead to huge losses either due to the time lost recovery from the incident, financial gained by the competing company who purchased the intellectual property that was stolen to get ahead or for financial gains.

d. **Cost of Cybersecurity Measures and increase in operational costs.** Business invest in security measures to mitigate against cybercrimes either post incident or as part of a larger project aimed addressing security gaps identified. This could be costs associated with software purchases, licenses, employment hires and trainings provided to members of staff.

e. **Impact on Employment.** Cybercrime can affect employment in various ways. On one hand, it

creates demand for cybersecurity professionals. On the other hand, it can lead to job losses in companies that suffer significant financial damage from cyber-attacks.

VIII. Strategies for combatting cybercrimes in Nigeria

Combatting cybercrimes require a multidimensional approach due to the complexities that has arisen as a result of the various causes of cybercrime in the society. There is the need to have this addressed through a combined approach of embedding technological advancements, educational perspective particularly as it regards training and awareness, regulatory policies enactment to address the menace of cybercrimes and collaborative strategies and partnerships.

a. Development of strong Legislation on cybercrime activities and government initiatives.

Implementation and enactment of legislative processes is one of the major ways of combating cybercrimes since this becomes the baseline of ensures consequences are meted out on the cybercriminals as backed by law. The Nigerian government took a major step via the establishment which was responsible for responding to cyber related incidents in 2007 and followed up with enacting series of cybersecurity acts, laws, guidelines and frameworks, some of which are as follows:

- **Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015.** Which provides the required framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria [57]
- **National Cybersecurity Policy and Strategy (NCPS) 2021.** Which is expected to foster cooperation with Nigerian international allies in security and economic development as well as ensure the protection of Nigeria's cyberspace from cyber-attacks, online fraud, and other related illicit activities such as fake news and hate speech. [58]
- **Nigeria Data Protection Regulation (NDPR), 2019.** This enforces data protection in Nigeria and acts as a guide in understanding the controls and measures to introduce in operations to comply with the legislation. [59]
- **Guidelines for Banking Industry on Cybersecurity Framework, 2018.** This was released by the central bank of Nigeria following an increase in the number and sophistication of cybersecurity threats and the need to strengthen their cyber defenses. [60]

- **Nigerian Communications Commission (NCC) Cybersecurity Guidelines.** Have issues various regulations and guidelines aimed at preventing cybercrimes as it relates to cybersecurity some of which include the below [61]
 - i. NCC Regulations on the Use of Short Messages Service (SMS) (2018)
 - ii. NCC Regulations on the Use of Short Messages Service (SMS) (2018)
- **National Information Technology Development Agency (NITDA) Guidelines.** NITDA has issued guidelines for the protection of data and enhancing cybersecurity in various sectors [61]
 - i. NITDA Guidelines for Management of Cybersecurity Incidents (2020)
 - ii. NITDA Guidelines for Cybersecurity in the Nigerian Financial Sector (2019)
 - iii. NITDA Guidelines for Data Protection (2019)
- **Advanced Fee Fraud and Other Related Offences Act, 2006.** This is an act to Prohibit and punish certain offences pertaining to Advance Fee Fraud and other fraud related offences and to repeal other Acts related therewith. *According to Section 23 of the advance fee fraud Act (Laws of the Federation of Nigeria, 2006): False pretence means a representation, whether deliberate or reckless, made by word, in writing or by conduct, of a matter of fact or law, either past or present, which representation is false in fact or law, and which the person making it knows to be false or does not believe to be true*
- **National Cybersecurity Centre (NCC) Directives**
 - i. NCC Directive on the Implementation of Two-Factor Authentication (2FA) (2020)
 - ii. NCC Directive on the Use of Secure Sockets Layer/Transport Layer Security (SSL/TLS) (2020)
- **Nigeria Criminal Code Act 1990.** This act criminalises any form of fraud or stealing and it becomes punishable under this act. This essentially covers cyber related crimes related to potential theft of funds among many others. For example section 419 clearly states obtaining under false pretence. *Section 419: Any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years.*

IX. Promoting Cybersecurity Awareness Programs

The lack of cybersecurity awareness is a major concern as it makes it easy for the malicious threat actors to carry out cybercrimes that affect and impact the economy which will go a long way in the reduction of cybercrime.

Various organizations, including government agencies, NGOs, and private companies, conduct awareness programs to educate the public and businesses about cyber threats and protective measures. For example NITDA, NCC, NCS have developed workshops, seminars, conferences and guidelines were developed and disseminated for creating awareness on cybersecurity.

It is also important to invest in cybersecurity training of stakeholders, cybercrime fighting agencies and legislative arm of the government which will lead to developments of ever evolving legal frameworks used for combatting cybercrimes and criminals [62]. Regular training programs for law enforcement agencies, and the establishment of specialised cybercrime units equipped with the latest technological tools and know-how [63]

Continuous public awareness campaigns are vital in educating individuals and businesses about cybersecurity. These campaigns should cover the latest cyber threats and provide practical tips on how to protect against them.

X. Active participation from Law Enforcement Agencies in the fight against cybercrime

The agencies enacted by law play a vital role in combating and prosecuting cybercriminals. This will serve a strong deterrent which will ultimately aid in the reduction of cybercrimes in the society at large.

Some law enforcement agencies include

- a. The specialized units within the Nigerian Police Force and other security agencies are tasked with investigating and prosecuting cybercrime cases.
- b. Economic and Financial Crimes Commission (EFCC)
- c. National Information Technology Development Agency (NITDA)
- d. Office of the National Security Adviser (ONSA) - National Cybersecurity Coordination Centre (NCCC)

e. Nigerian Communications Commission (NCC)

f. Independent Corrupt Practices and Other Related Offences Commission (ICPC)

XI. Implementation of Technological Solutions and enhancing digital forensics capabilities

With the ever evolving sophistication of cyber-attacks and threat actors, there is the need to implement technological solutions aimed at defending and combatting against the cyber threats. This will range from Intrusion detection systems, firewalls, anti-virus AV solutions, SIEM among many others. Continuous innovation and updating of these technologies are necessary to keep pace with evolving threats.

The establishment of cyber defenses response and forensics units will also play a critical role in drastically combatting cyber-attacks via detection and response mechanisms. There is also the need to equip the centre created such as the forensics units with advanced forensics tools and provide the requisite ongoing trainings to keep up with evolving threats.

XII. Strengthening International Cooperation and Collaboration to combat cybercrime

Cybercrime is a global pandemic and there is the need for international collaborations across borders to jointly combat and have this reduced drastically since the impact is felt internationally also.

Collaboration could be via the creation of working groups to enhance threat intelligence sharing, improve ways of carrying out cyber relates incidents investigations, participating in international cybersecurity forums and capacity building as the case may be.

For example an African joint operation against cybercrime project has been set up by the INTERPOL with timeframe going from 2024 to 2025. The project aims to further enhance the capabilities of national law enforcement agencies in Africa. This will be achieved through continued focus on preventing, detecting, investigating, and disrupting cybercrime activities. [64]

XIII. Developing Cybersecurity Skills

Building a skilled cybersecurity workforce is essential. Educational institutions should offer

specialized cybersecurity programs, and businesses should provide ongoing training for their employees.

There is need for the government to allocate funding and budgetary allocations geared towards advancing cybersecurity research and methodologies aimed at supporting academic institutions to deepen and develop cybersecurity programs and courses to

This could also be via the creation of cybersecurity hubs aimed providing training, resources encouraging the development of cybersecurity start-ups and innovation through grants and incentives.

XIV. Conclusion

Cybercrime and cyber related attacks poses a major challenge for Nigeria, impacting individuals, businesses and the national economy. This document highlights the pervasive trend of cybercrime, highlights cyber-attacks that have occurred against businesses in the Nigeria space and explores its economic impact and the measures to combat these threats.

Significant progress has already been made, but much more remains to be done. With improved legislation, increased public awareness, stronger public-private partnerships, investment in cybersecurity infrastructure, development of cybersecurity skills and increased international cooperation, Nigeria can effectively combat cybercrime and mitigate its economic impact.

References

[1] Akeem Olalekan Ayub, Linus Akor, "Trends, Patterns and Consequences of Cybercrime in Nigeria", *Gusau International Journal of Management and Social Sciences*, Vol. 5 No. 1 (2022)

[2] (2022) Citation Cyber Formerly Cmitigate [Online]. Available: <https://mitigatecyber.com/the-economic-impacts-of-cyber-crime-how-it-costs-us-all/>

[3] Chiemeke Stella, Imafidor Omokhagbo, "An assessment of the impact of digital technology adoption on economic growth and labour productivity in Nigeria", *NETNOMICS: Economic Research and Electronic Networking* 21(2), 2020

[4] Gyamfi Emmanuel Kojo et al, "A Comprehensive Analytical Review on Cybercrime in West Africa", 2024

Available:

<https://arxiv.org/html/2402.01649v1#bib.bib1>

[5] Albrecht et al, "The use of cryptocurrencies in the money laundering process", *Journal of Money Laundering Control*, Vol 22, 2019

[6] (2019) NDIC Quarterly Vol 34 No 12. [Online] Available: <https://ndic.gov.ng/wp-content/uploads/2020/08/NDIC-Quarterly-Vol-34-No-12-2019-Article-The-Impact-Of-Cybercrime-On-The-Nigerian-Economy-And-Banking-System.pdf>

[7] Henry Osborn Quarshie , Alexander Martin-Odom , "Fighting Cybercrime in Africa", *Computer Science and Engineering*, Vol. 2 No. 6, 2012, pp. 98-100. doi: 10.5923/j.computer.20120206.03.

[8] (2022) Cybercrime in West Africa: towards a multi-state organisation? Available: <https://incyber.org/en/article/cybercrime-in-west-africa-towards-a-multi-state-organisation/>

[9] (2020) Cyber Security Breaches Survey 2020 [Online] Available: <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020>

[10] (2023) Simplilearn: What is Phishing Attack in Cyber Security - Complete Guide [Online] Available: <https://www.simplilearn.com/tutorials/cryptography-tutorial/what-is-phishing-attack>

[11] Phishing [Online] Available: <https://www.knowbe4.com/resource-center/phishing>

[12] Muntode, Antonette, "An Overview on Phishing- its types and Countermeasures", *International Journal of Engineering Research and* V8(12), 2019

[13] (2021) EMAIL SECURITY:10 Phishing Email Examples You Need to See, BY SAVVY SECURITY [Online] Available: <https://cheapsslsecurity.com/blog/10-phishing-email-examples-you-need-to-see/>

[14] (2023) Spear Phishing vs. Whaling [Online] Available: <https://www.infosectrain.com/blog/spear-phishing-vs-whaling/>

- [15] WHALING: The highly targeted form of phishing that targets executives [Online] Available: <https://www.meshsecurity.io/whaling>
- [16] Pharming TechTarget Contributor [Online] Available: <https://www.techtarget.com/searchsecurity/definition/pharming>
- [17] (2023) What Is Smishing? Definition, Types of Attacks, Protection Measures, and More. [Online] Available: <https://heimdalsecurity.com/blog/what-is-smishing/>
- [18] Mangut Palang, Aristarkus Datukun, "The Current Phishing Techniques – Perspective of the Nigerian Environment", *World Journal of Innovative Research*, 2021, Vol 10
- [19] (2023) What's the Difference between Smishing and Vishing? [Online] Available: <https://www.terranosecurity.com/blog/how-to-recognize-smishing-and-vishing-attacks>
- [20] (2024) what is Vishing and How To Protect Yourself? Available: <https://clearvpn.com/blog/what-is-vishing/>
- [21] Victoria Wang, Harrison Nnaji & Jeyong Jung, "Internet Banking in Nigeria: Cyber Security Breaches, Practices and Capability" [Online] Available: https://pure.port.ac.uk/ws/portalfiles/portal/21217684/Manuscript_Internet_Banking_in_Nigeria.pdf
- [22] Aliyu Ahmed et al, "An Integrated Framework for Detecting and prevention of Trojan Horse (BINGHE) in a Client-Server Network", *International Journal of Innovative Research in Science, Engineering and Technology*, 2014
- [23] Fortinet: What is a Trojan Horse Virus? [Online]. Available: <https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus#:~:text=A%20Trojan%20Horse%20Virus%20is,system%20access%20with%20their%20software>
- [24] Aurangzeb Sana et al, "Ransomware: A Survey and Trends", *Journal of Information Assurance and Security (ESCI - Thomson Reuters Indexed)*, ISSN: 1554-10, 2017
- [25] Bhattacharya, S., and C. R.S. Kumar. 2017. "Ransomware: The CryptoVirus Subverting Cloud Security." 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies, ICAMMAET 2017 2017–Janua: 1–6
- [26] Fortinet: What Is Spyware? [Online] Available: <https://www.fortinet.com/resources/cyberglossary/spyware>
- [27] A.Prakasha et al, "Detection and Mitigation of Denial of Service Attacks Using Stratified Architecture", 4th International Conference on Recent Trends in Computer Science & Engineering, 87 (2016) 275 – 280
- [28] CloudFlare: What is a DDoS attack? [Online] Available: <https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-attack/>
- [29] Akamai: What Is a Volumetric Attack? [Online] Available: <https://www.akamai.com/glossary/what-is-a-volumetric-attack>
- [30] Onelogin: What is a DDoS Attack? Types, Prevention, and Remediation [Online] Available: <https://www.onelogin.com/learn/ddos-attack>
- [31] (2023), CyberCrowd: Unmasking the hidden danger: Insider Threats in Cyber Security [Online] Available: <https://www.cybercrowd.co.uk/news/unmasking-the-hidden-danger-insider-threats-in-cyber-security/>
- [32] (2020), ProofPoint: 2020 COST OF INSIDER THREATS GLOBAL REPORT [Online] Available: https://www.proofpoint.com/sites/default/files/obse-rveit/2020/02/2020-Global-Cost-of-Insider-Threats-Ponemon-Report_UTD.pdf
- [33] FATOKI JACOB, "The influence of cyber security on financial fraud in the Nigerian banking industry", *International Journal of Science and Research Archive*, 2023
- [34] (2022) QUARTZ: MTN's mobile money push into Nigeria was hacked for millions within days [Online] Available: <https://qz.com/africa/2183438/mtn-nigerias-momopsb-is-suing-banks-after-53-million-breach>

[35] (2022) TheCable: ‘Security breach’: MTN subsidiary heads to court, seeks refund of N22bn from 18 banks [Online]

Available: <https://www.thecable.ng/security-breach-mtn-subsi-dary-heads-to-court-seeks-refund-of-n22bn-from-18-banks/>

[36] (2024) ITEdgeNews: NDPC probes MTN’s MoMo PSB over privacy breach [Online] Available: <https://www.itedgenews.africa/ndpc-probes-mtns-momo-psb-over-privacy-breach/>

[37] (2022) MoMo PSB Statement [Online] Available: <https://momo.mtn.com/wp-content/uploads/sites/15/2022/06/MoMo-PSB-Statement.pdf>

[38] (2023) Nairametrics: Patricia suffers massive losses in crypto assets after security breach [Online] Available: https://nairametrics.com/2023/05/28/patricia-suffers-massive-losses-in-crypto-assets-after-security-breach/#google_vignette

[39] 2023, x.com Downtime Update [Online] Available: <https://x.com/PatriciaSwitch/status/1662049215772516352/photo/1>

[40] (2023) Punchng: Babcock university confirms hack of school website [Online] Available: <https://punchng.com/babcock-university-confirms-hack-of-school-website/>

[41] (2016) Okay: Hackers Take Over FUTA Official Website [Online] Website: <https://www.okay.ng/photo-hackers-take-over-futa-official-website/>

[42] (2016) Nairaland: FUTA Website Has Been Hacked Again [Online] Website: <https://www.nairaland.com/3446852/futa-website-been-hacked-again>

[43] (2015) Channelstv: INEC Restores Hacked Website [Online] Website: <https://www.channelstv.com/2015/03/28/inec-restores-hacked-website/>

[44] (2015) X.com: INEC Nigeria Update [Online] Available: <https://x.com/inecnigeria/status/581771140403765248?lang=en>

[45] (2019) lindaikejsblog: University of Nigeria, Nsukka (UNN) official website hacked by suspected

French hacker [Online] Available: <https://www.lindaikejsblog.com/2019/10/university-of-nigeria-nsukka-unn-official-website-hacked-by-suspected-french-hacker.html>

[46] (2020) DailyPost: N2.5bn fraud: Union Bank hackers to cool off in prison [Online] Available: <https://dailypost.ng/2020/07/03/n2-5bn-fraud-union-bank-hackers-to-cool-off-in-prison/>

[47] (2021) cyberplural: TOP BREACHES (2015 - 2021) [Online] Available: https://blog.cyberplural.com/wp-content/uploads/2021/05/CyberPlural_Top5-2.pdf

[48] (2018) TheCable: ALERT: Did you book an Arik flight online in 2017? Your data might have leaked [Online] Available: <https://www.thecable.ng/data-belonging-to-thousands-of-arik-passengers-might-have-been-compromised/>

[49] (2018) ZDNET: Nigerian airline Arik Air may have leaked customer data [Online] Available: <https://www.zdnet.com/article/nigerian-airline-arik-air-may-have-leaked-customer-data/>

[50] (2020) TroyHunt: The Difficulty of Disclosure, Surebet247 and the Streisand Effect [Online] Available: <https://www.troyhunt.com/the-difficulty-of-disclosure-surebet247-and-the-streisand-effect/>

[51] (2021) technext24: amb Isn’t the First! Here are 10 times Nigerian Govt Agencies have Been Hacked in the Last Decade [Online] Available: https://technext24.com/2021/04/15/jamb-isnt-the-first-here-are-10-times-nigerian-govt-agencies-have-been-hacked-in-the-last-decade/#google_vignette

[52] (2022) yinksmedia: Bet9ja Website Hacked by Russian BlackCat Group: What you need to know? [Online] Available: <https://yinksmedia.com/bet9ja-criminal-cyber-attack-what-you-need-to-know/>

[53] (2022) Tripwire: BlackCat ransomware - what you need to know [Online] Available: <https://www.tripwire.com/state-of-security/blackcat-ransomware-what-you-need-to-know>

[54] (2022) halcyon: alphv attacks bet9ja.com | goldbet.it [Online] Available: <https://www.halcyon.com/alphv-attacks-bet9ja-com-goldbet-it>

[55] (2022) Nairaland: Bet9ja Hack [Online]

Available:

https://www.nairaland.com/attachments/15235255_fbimg1649359040177_jpega68336b780340fb72ae709bb1a0b89b8

[56] Hassan A. B., Lass F. D. and Makinde J. (2012): Cybercrime in Nigeria: Causes, Effects and the Way Out, *ARNP Journal of Science and Technology*, vol. 2(7), 626 – 631

[57] NFIU, CYBERCRIMES (PROHIBITION, PREVENTION, ETC) ACT, 2015 [Online]

Available:

<https://www.nfiu.gov.ng/images/Downloads/downloads/cybercrime.pdf>

[58] (2021) apiintelligence: NATIONAL CYBERSECURITY POLICY & STRATEGY [Online]

Available:

<https://api.apiintelligence.org/upload/4650ae0b15daf1e5c3fac12e93cbde610.pdf>

[59] (2019) NITDA: NIGERIA DATA PROTECTION REGULATION 2019: IMPLEMENTATION FRAMEWORK [Online]

Available:

<https://nitda.gov.ng/wp-content/uploads/2021/01/NDPR-Implementation-Framework.pdf>

[60] (2018) cbn: RISK-BASED CYBERSECURITY FRAMEWORK AND GUIDELINES [Online]

Available:

<https://www.cbn.gov.ng/out/2018/bsd/risk%20base%20cybersecurity%20framework%20exposure%20draft%20june.pdf>

[61] (2024) Cybersecurity Regulations in Nigeria: What You Need to Know [Online]

Available: <https://www.linkedin.com/pulse/cybersecurity-regulations-nigeria-what-you-need-know-basirat-jimoh-npyqf>

[62] Alabi, Marvellous, Literature Review on Cybersecurity in Nigeria (May 6, 2024). Available at SSRN: <https://ssrn.com/abstract=4818514> or <http://dx.doi.org/10.2139/ssrn.4818514>

[63] (2023) THE IMPACT OF CYBERCRIME AND CYBERSECURITY ON NIGERIA'S NATIONAL SECURITY [Online]

Available: <https://dspace.cuni.cz/bitstream/handle/20.500.11956/187353/120460718.pdf?sequence=1&isAllowed=y>

[64] AFJOC - African Joint Operation against Cybercrime [Online]

Available: <https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations/AFJOC-African-Joint-Operation-against-Cybercrime>

bercrime-operations/AFJOC-African-Joint-Operation-against-Cybercrime

[65] NIST Information Technology Laboratory, COMPUTER SECURITY RESOURCE CENTER Available:

<https://csrc.nist.gov/glossary/term/phishing#:~:text=Definitions%3A,legitimate%20business%20or%20reputable%20person>