**Open Access Library Journal**
2025, Volume 12, e13218
ISSN Online: 2333-9721
ISSN Print: 2333-9705

# Cybercrime in Developing Countries: Negative Effects and Panacea

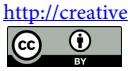
**John Otozi Ugah[1], Onu Sunday[2], Alozie Obidinma[3], Ori Silas Ene[2]**

[1]Department of Computer Science, Ebonyi State University, Abakaliki, Nigeria
[2]Department of Computer Science, David Umahi Federal University of Health Sciences, Uburu, Nigeria
[3]Department of Mathematics/Computer Science, Clifford University, Owerrinta, Nigeria
Email: onus@dufuhs.edu.ng

**How to cite this paper:** Ugah, J.O., Sunday, O., Obidinma, A. and Ene, O.S. (2025) Cybercrime in Developing Countries: Negative Effects and Panacea. *Open Access Library Journal*, **12**: e13218.
https://doi.org/10.4236/oalib.1113218

**Received:** March 6, 2025
**Accepted:** April 7, 2025
**Published:** April 10, 2025







## Abstract

Cybercrime could be described as criminal activities carried out using a computer, network, or any other known digital device. Some of these activities include unethical hacking, phishing, identity theft, ransomware, malware attacks, and software piracy, among many others. This heinous crime has been on a geometric rise in recent times in developing countries. This study explores cybercrimes in developing countries, various forms, negative effects, and the panacea to the ugly menace. In order to achieve this, an empirical study was carried out using a questionnaire from Google Form. Seventy individuals from different works of life in different States in Nigeria responded actively to the survey. Thus, it was easy to represent their feedback using some popular statistical tools like pie chart, a simple bar chart and percentages. This research work shows that indeed, cybercrime has eaten deep into the fabrics of developing countries and needs to be checkmated. This study will educate the populace in developing countries about the various negative effects and the solution to the impact of this illicit digital crime. It also exposed the flaws of individuals, private and public sectors, in compliance with standard cybersecurity measures. Above all, it was discovered that cybersecurity awareness in developing countries is actually below standard; hence, there is a need to intensify the process to curb or probably ameliorate the negative effects of cybercrimes in developing countries.

## Subject Areas

Computer and Network Security

## Keywords

Cybercrime, Cybersecurity, Negative Effects, Panacea, Survey Methodology

## 1. Introduction

In the current world setting, where systems and businesses are interconnected thereby making it a global village, and technological innovations are advancing at an enormous rate, the threat of cybercrime has a corresponding increase alarmingly and poses a serious challenge for governments, businesses, and citizens alike. The range and complexity of attacks have grown exponentially in recent years, with criminals exploiting new methods of infiltration in order to access confidential data and sensitive information [1].

As this trend continues unchecked, the security risks for all organizations, both public and private sectors, are greatly increased, at an immeasurable cost to the global economy.

An article published by the World Economic Forum's Centre for Cybersecurity stated that "nearly half of businesses are being hit by economic crime, with cybercrime the gravest threat" [2].

Africa has been among the fastest growing regions in terms of cybercrime activities. The continent is also a source of significant cyber-attacks targeting the rest of the world. However, a number of measures have been taken to address cyber-threats and improve cyber-security in the continent. Many countries in the continent have developed legislation to fight cyber-threats. They have also strengthened enforcement measures. Efforts have also been undertaken by the private sector to strengthen cyber-security [3]. Note also that cybercrime is a growing concern in West Africa due to the increasing use of technology and internet penetration in the region. West African countries face significant cybercrime challenges, exacerbated by inadequate resources and a dearth of security experts [4]. Cybercrime is popularly referred to as Yahoo Yahoo, Yahoo plus or in Igbo local parlance as oke-iteh in Nigeria [5]. Cybercrime, could be seen as a crime committed with phones and/or a computer through a communication device or a transmission medium referred to as the "cyberspace" and a global network called the "internet" [6]. Thus, cybercrime has been complex and the costs have been going up since corporations, governments, individuals, or people all over the world started using computers to do business. [7] Opined that any criminal offense committed using the internet or another computer network as a component of the crime is adjudged to be cybercrime. [8] argued that cyber-crimes constitute offenses done against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or using indirect modern communication networks such as the internet and mobile devices/phones, such crimes may threaten the nation's security and financial health. Cybercrime is now committed by people of all ages, from young to old, but most often by undergraduates [9]. As we advance toward the 21st century, it can be observed that the technological innovations have laid the way for the entire population to use computer technology to gather and organize large amounts of information. While computer technology has opened doors to enhanced conveniences for mankind, this same technology has also opened new doors for criminals

This study conducted a systematic literature review focusing on prevalence of cybercrime, governing policies, regulations, and methodologies for combating cybercrime in developing countries. It pinpoints potential cybercrime prevention strategies. Our findings highlight the urgency for policymakers and law enforcement agencies to devise more efficient prevention strategies and policies.

## 2. Motivation for the Study

Security threats have a gigantic menace bedeviling Developing Countries over the years. With innovations in technology and the internet, most businesses, government and individuals have embraced the current trend. But such innovations are not devoid of serious threats. Cybercrime is a major threat to both public and private sectors. Financial institutions have spent whooping sum of money to fight this trend. Businesses and lives have been lost, identities stolen, reputations damaged and so on, due to this ugly menace. The government is not left behind in being targeted by cybercriminals. Security documents are targeted and cyber espionage is used to steal vital information to either threaten the State, demand for ransom, or to cripple the State. Also, cybercrime is used to commit acts of terrorism. This makes the government spend heavily in order to manage this menace and to guard information that would be deadly in the wrong hands. As a result of the above, this research investigates cybercrime in developing countries, its negative effects, and the panacea for ending or reducing its impact.

## 3. Review of Related Literature

In recent years, there has been a significant increase worldwide in the number of incidents related to cybercrime, and West Africa is no exception [10]. According to various reports and analyses, West African countries have experienced a surge in cybercrime activities, with major incidents including phishing scams, ransomware attacks, financial fraud, identity theft, and online scams. These criminal activities have impacted both individuals and businesses and local, regional, and international economies within the sub-region, leading to a significant decrease in trust and confidence in online transactions and financial activities [3] [11]. Computer security experts have found that a significant amount of cybercrime originates in Africa, and this poses a severe threat due to the inadequate protection of computer systems [12]. Unfortunately, poverty and underdevelopment are the primary causes of the growth of cybercrime in the region, making it crucial to have a coordinated approach to combat these threats.

## 4. Types of Cybercrime

From our research across different sources and authors, the following are the types of cybercrime prevalent in developing countries: Phishing, Malware, Identity theft, Cyberstalking, Hacking, Cyber-terrorism, phishing [13].

According to [14], phishing is a fraudulent practice in which an attacker impersonates or masquerades as a reputable entity or person in an email or other form

of communication. It also impersonates a legitimate company or individual to tick users into revealing sensitive information [15]. Attackers commonly use phishing emails to distribute malicious links or attachments that can extract login credentials, account numbers and other personal information from victims. Malicious software (malware) is any intrusive software developed by cybercriminals (often called hackers) to steal data and damage or destroy computers and computer systems. Examples include viruses, worms, Trojan virus, spyware, adware, ransomware, etc. [16] [17]. The intent of malware is to cause havoc and steal information or resources for monetary gain or for sheer sabotage. This occurs when a criminal gains access to a user's personal information to steal funds, access confidential information, or participate in tax or health insurance fund [18]. They can open a phone/internet account with the stolen identity, use identity to plan criminal activity, etc. This is when a cybercriminal uses email, direct messaging, or other electronic means to harass, scare, or threaten someone with physical harm [19]. This is unauthorized access to a computer system or account, often to inflict further damage on the target [15]. Cyberterrorism: This is the use of the internet to conduct violent acts that result in, or threaten, the loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation [17].

## 5. Negative Effects of Cybercrime

The following are the negative effects of cybercrime:

(1) Reputational Damage
(2) Financial Loss
(3) Psychological Trauma
(4) Identity Theft
(5) Data Breach

**Reputational Damage:** This occurs when sensitive customer data is leaked or stolen. This leads to loss of trust and negative publicity that could damage its brand and reputation [18].

**Financial Loss** Cybersecurity breaches can result in various financial losses for businesses. These include the cost of mitigating the breach, such as hiring experts to investigate and repair the damage, notifying customers and settling legal claims. It can also lead to loss of revenue from delayed or cancelled projects and reputational damage if sensitive customer data are leaked, companies may also face hefty fine from the government regulators if they fail to meet minimum security requirements. The company may even close in extreme cases [20].

**Psychological Trauma:** The emotional and psychological impact of cyberattack on individuals can range from mild to severe and lead to symptoms of depression, anxiety, panic attacks, posttraumatic stress, and even suicide. Individual victims are left with scars from emotional trauma like a sense of violation, powerlessness, anxiety, depression, and eating/sleeping disorder. Survivors of cyberattack can go on to experience lingering feelings of guilt, shame and grief. They can also be left feeling robbed and afraid of another attack [20].

**Identity Theft:** This occurs when criminals steal a victim's personal information to commit criminal acts. Using this stolen information, a criminal takes over the victim's identity and conducts a range of fraudulent activities in their name. It also occurs when a criminal gains access to a user's personal information to steal funds, access confidential information, or participate in tax or health insurance fund [18]. They can open a phone/internet account with the stolen identity, use identity to plan a criminal activity, etc.

**Data Breach:** This is any security incident in which unauthorized parties access sensitive or confidential information, including personal data (bank account details, healthcare data, and so on) and corporate data (customer records, intellectual property, financial information, and so on) [21].

Other negative effects of cybercrime are: Loss of Life, Altered Business Practices, Compromised Records, and System Crash

## 6. Causes of Cybercrime in Developing Countries

Increasing cyberattacks in the continent can be attributed to vulnerable systems and lax cybersecurity practices. According to Business Software Alliance, two countries with the world's highest software piracy rates in 2017 were from Africa: Libya and Zimbabwe. The proportions of unlicensed software in the two countries were 90% and 89% respectively [3].

Since pirated software products cannot take advantage of updates from manufacturers, they accelerate the spread of malware. Cybersecurity is considered to be as a luxury, not a necessity in many African economies. Its importance has not yet been sufficiently appreciated or acknowledged in the continent.

Cybersecurity budgets in many organizations are reported to be less than 1% and many organizations had a zero-budg *et al.* located to cybersecurity [22]. Even financial institutions, which face biggest cyber-threats, lack proper cybersecurity practices. One study in 2009 showed that 60% of Kenyan banks had insecure systems. According to a 2011. Deloitte study, only 40% of banks in Kenya, Uganda and Tanzania were prepared against cyber-threats (Karambu, 2011).

Another survey conducted among banks in Kenya, Rwanda, Uganda, Tanzania and Zambia revealed that banks were at high risk from threats, such as hacking, employees with poor sense of security, malicious insiders.

Another problem is related to the lack of skills among Internet users to protect themselves from rapidly rising cyber-threats [23]. Just like in other developing countries, many African Internet users are inexperienced and not technically savvy. A high proportion of them are getting computers and connecting to the Internet for the first time. A majority of them also lack English language. This later point is crucial due to the fact that most of the information, instructions, and other contents for security products are available in English language only. Many African Internet users cannot use cybersecurity products developed in English language. The continent faces a severe shortage of cybersecurity manpower. It is estimated that Africa will have a shortage of 100,000 cybersecurity personnel by 2020.5 Just

like in the BRICS countries (Brazil, Russia, India, China, and South Africa) [23]. African economies have faced economic and institutional barriers in developing cybersecurity manpower. For instance, Cameroon which is among the countries worst affected by cybercrime in Africa, was reported to be facing a dilemma to take measures to address the problem. It was reported in 2016 that policy makers in the country were in the process of launching cybersecurity skill development programs. Policy makers, however, feared that after completing the training program, the trainees could use the skills gained to commit cybercrimes [3].

A final reason concerns weak legislation and law enforcement [3]. Most African economies are characterized by permissiveness of regulatory regimes that provide a fertile ground for cybercrime activities. According to a November 2016 report of the African Union Commission (AUC) and the cybersecurity firm Symantec, out of the 54 countries of Africa, 30 lacked specific legal provisions to fight cybercrime and deal with electronic evidence. Law enforcement officials in some countries do not take major actions against hackers attacking international websites. For instance, it was reported that government officials in Nigeria claimed that they were ignorant of cybercrimes originating from the country and some labeled it as Western propaganda. Some elected high-level State officials were also reportedly involved in cybercrimes. In 2003, Nigeria's Economic and Financial Crimes Commission (EFCC) arrested Maurice Ibekwe, a member of Nigeria's House of Representatives for his alleged engagement in cybercrime-related activities [22].

## 7. Cybersecurity: A Panacea to the Negative Impact of Cybercrime

Cybersecurity is the practice of protecting internet-connected systems such as hardware, software and data from cyberthreats. It is used to protect against unauthorized access to data centers and other computerized systems. [24] this can provide a strong security posture against malicious attacks designed to access, alter, delete, destroy or extort an organization's or user's systems and sensitive data. It has the following benefits:

(1) Protection against cyberattacks and data breaches.
(2) Protection of data and network.
(3) Prevention of unauthorized user access.
(4) Improved recovery time after a breach.
(5) Protection for end users and endpoint devices.
(6) Regulatory compliance.
(7) Business continuity.
(8) Improved confidence in company's reputation and trust.

## 8. Cybersecurity Measures

According to [25] the following are the cybersecurity measures:

(1) Maintain an accurate inventory of control system devices and eliminate any exposure of this equipment to external networks.

(2) Implement network segmentation and apply firewalls.

(3) Use secure remote access methods.

(4) Establish role-based access controls and implement system logging.

(5) Use only strong passwords, change default passwords, and consider other access controls.

(6) Maintain awareness of vulnerabilities and implement necessary patches and updates.

(7) Develop and enforce policies on mobile devices.

(8) Implement an employee cybersecurity training program.

(9) Involve executives in cybersecurity.

(10) Implement measures for detecting compromises and develop a Cybersecurity Incident Response Plan.

## 9. Cybersecurity Tools

Cybersecurity tools help you monitor and fix potential security concerns [26]. These tools are aiding companies and individuals in maintaining their online privacy and security. They continuously monitor computer systems or networks and warn the user of potential risks the moment it detects it.

Below are the types of cybersecurity tools [27]

(1) Network security monitoring tools—used to identify external network threats by detecting and preventing attacks that originate from organization's intranet.

(2) Security compliance tools—scans the network and processes to detect non-compliant activities and security failures and notifies system administrators to take corrective actions.

(3) Web vulnerability scanning tools—continuously monitor potential risks of web applications to reveal security flaws and vulnerabilities.

(4) Network defense wireless tool—protects data while maintaining network's usability and integrity.

(5) Encryption tools—decode and encode streams of data that are at rest or in transit, making them safe and unreadable by unauthorized individuals.

(6) Firewalls—prevents unauthorized users from accessing the intranet.

(7) Packet sniffers—helps to discover apps that gather data for security analysis

(8) Antivirus system—helps to monitor, block and remove viruses as well as other malware from the system.

Other tools are: Managed detection and response services, Public key infrastructure services and Penetration testing.

The following are the top 16 cybersecurity tools [27]: Sprinto, Kali Linux, Cain and Abel, Metasploit, John the Ripper, Wireshark, Nikto, Topdump, KisMAC, NetStumbler, Splunk, Forcepoint, Aircrack-ng, Nexpose, Nessus Professional, and N Map.

## 10. Fight Against Cybercrimes in Nigeria

In 2015, the Nigerian government signed into law the cybercrimes (Prohibition,

Prevention, Etc) Act, 2015 as an effective, unified, and comprehensive legal, regulatory, and institutional framework for the prohibition, prevention, detection, prosecution, and punishment of cybercrimes in Nigeria. According to the Act's explanatory Memorandum, the instrument was also enacted to ensure the protection of critical national information infrastructure and promote cyber security, the protection of computer systems and networks, electronic communications, data, computer programs, intellectual property, and privacy rights.

Below are laws and acts enacted to fight against cybercrime in Nigeria

(1) The 1999 Constitution of the Federal Republic of Nigeria (as amended) ("CFRN").

(2) The cybercrimes (Prohibition and Prevention, Etc.) Amendment Act, 2024.

(3) Nigeria Data Protection Act, 2023 ("NDPA").

(4) Nigeria Data Protection Regulation, 2019 ("NDPR").

(5) Nigeria Data Protection Regulation Implementation Framework, 2020.

(6) The Advance Fee Fraud and other Related Offences Act, 2006 ("AFF").

(7) Terrorism (Prevention and Prohibition) Act, 2022.

(8) The Economic and Financial Crimes Commission (Establishment, etc.) Act, 2004.

(9) The Money Laundering (Prevention and Prohibition) Act, 2022.

(10) Nigerian Communications Communication Act, 2003.

(11) The NCC Guidelines for the Provision of Internet Service.

(12) Nigeria Bar Association Cybersecurity Guideline, 2024.

(13) Designation and Protection of Critical National Information Infrastructure Order, 2024.

(14) Risk-Based Cybersecurity Framework and Guidelines for Other Financial Institutions, 2022.

The following are some of the penalties for committing cybercrime in Nigeria.

**Hacking (*i.e.* unauthorised access)**: Section 6 of the cybercrimes (Prohibition and Prevention etc.) (Amendment) Act 2024 (the "Cybercrimes Act") makes it an offence for any person, without authorisation, to intentionally access a computer system in whole or in part, for fraudulent purpose in order to obtain data vital to national security. The maximum penalty for this offence in Nigeria is imprisonment for a term of not more than five years, a fine of not more than ₦5 million, or both such fine and imprisonment.

**Denial-of-service attacks**: Section 8 of the Cybercrimes Act makes it an offence for any person without lawful authority, intentionally or for fraudulent purposes to carry out an act that causes directly or indirectly, the serious hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or any other form of interference with the computer system, which prevents the computer system or any part thereof, from functioning in accordance with its intended purpose. The maximum penalty for such offence is imprisonment for a term of not more than two

years, a fine of not more than ₦5 million, or both such fine and imprisonment.

**Phishing**: Under Section 32 of the Cybercrimes Act, it is an offence for anyone to attempt to obtain sensitive information such as usernames, passwords, or credit card details by masquerading as a trustworthy entity in electronic communications. This includes using emails or instant messaging to impersonate, and deceive users to change their password, or disclosing their identity with the intent of later using this information to commit fraud. The maximum penalty for this offence is imprisonment for a term of three years, a fine of ₦1 million, or both.

## 11. Research Questions

This research is geared towards answering the following questions:

**Q1.** What could be the possible causes for increased cases of cybercrime in developing countries?

**Q2.** What are the possible negative impacts of cybercrime in developing countries?

**Q3.** What is the best way to stop cybercrime in developing countries?

## 12. Materials and Methods

The methods used for this research work are the use of questionnaire and interviews. Questionnaires were designed in line with the objectives and aim of the study as appropriate. Open-ended questions were constructed in line with the perspective of the respondents and interview were used for data collection. Researchers developed questionnaire on the basis of literature and related researches. Surveys were used to gather information from the respondents.

**Study Scope**: The study area comprises a random sampling of Civil Servants, Senior Health Professionals who are Tech experts in Nigeria, as well as students in some select tertiary institutions in the country of which 5.7% are people within 18 - 24 years, 38.6% were individuals in the age limit of 25 - 34years, 47.1% are in the range of 35 - 44 years and 8.6% fell between 45 - 54 years. This age distribution covers the individuals that are still active in service and may be affected by cybercrimes due to their day-to-day relationships.

## 13. Study Population

Google form was used to prepare the questionnaire. This was distributed to numerous WhatsApp platforms. At the end of the day, seventy (70) respondents filled and submitted their responses.

**Justification for Sample Size:**

The sample size is limited to the scope of the study. A sample size of 70 respondents was used based on a balance between achieving sufficient statistical power to detect meaningful effects while managing practical constraints like time, cost, and accessibility of the target population. This sample size allows for reliable analysis without becoming overly burdensome to collect data.

**Study Design:**

Stratified Random Sampling was used: The population was divided into sub-groups (strata) based on their age distributions, then a random sample was drawn from each stratum.

## 14. Data Collection Methods

Data for this study were collected through both primary and secondary sources. Materials from various books, web pages, and journals were reviewed, survey were conducted using questionnaire distributed via Google Forms and through interviews. The use of questionnaire ensures confirmation and completeness of data as well as increase confidence in the credibility of our findings. Stratified random sampling was employed to ensure a representative and comprehensive understanding of the research topic. The researchers collected the data from the respondents through Google form link which was shared via social media channels and groups or forums and direct from the interview after the distribution of questionnaires was done after the collection of data.

## 15. Data Analysis

To analyze the data collected from the respondents, statistical tools as pie-chart, histogram and percentage were used by the researchers. Descriptive Statistics was used to summarize the data using measures like percentage, histogram, and piechart.

## 16. Results

Surveys were used to gather information from 70 resident citizens of a developing country of which 5.7% are people within 18 - 24years, 38.6% were individuals in the age limit of 25 - 34years, 47.1% are in the range of 35 - 44years and 8.6% fell between 45 - 54 years as shown in Figure 1.

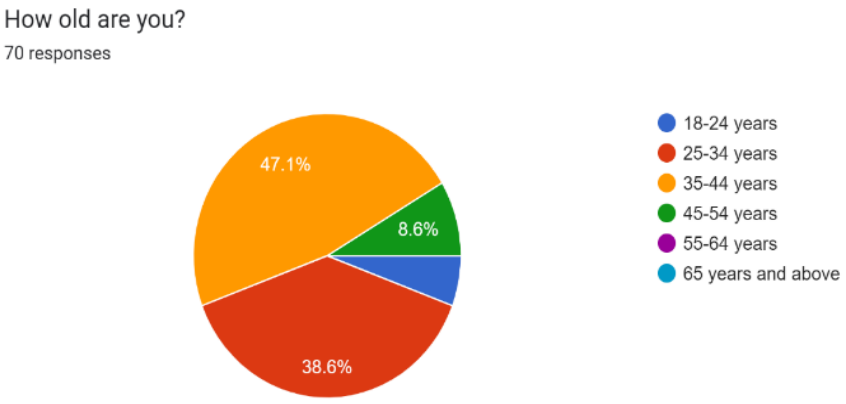



Figure 1. Age distribution of respondents.

The constituents of this sample size include individuals from different realms of life who are either employed, not gainfully employed or students as illustrated

in Figure 2 who were limited to one response. Their gender were 58.6% male and 41.4% female.

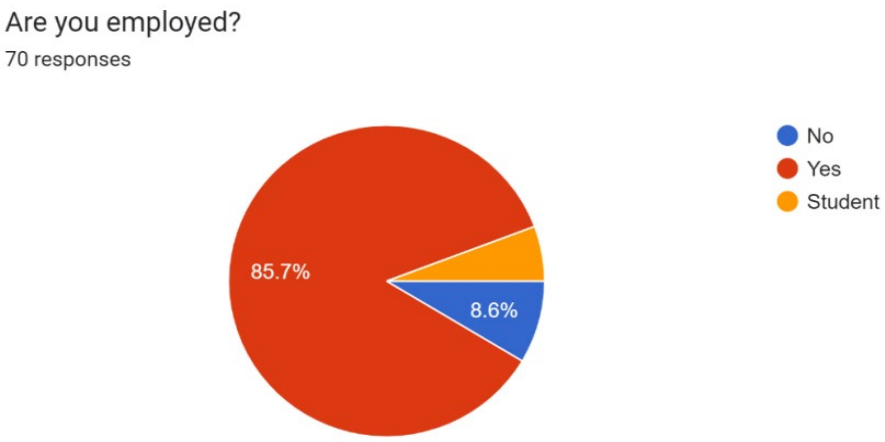



Figure 2. Economic status of respondents.

The questionnaire is in three major sections of Bio Data, Exposition and Compliance. The survey respondents were small but informative and accurate because the instrument was reviewed before.

The impacts of cybercrime are on the rise as 40% of the respondents admitted to have experienced hijacking of their social media accounts or probably emails. This is illustrated in Figure 3.

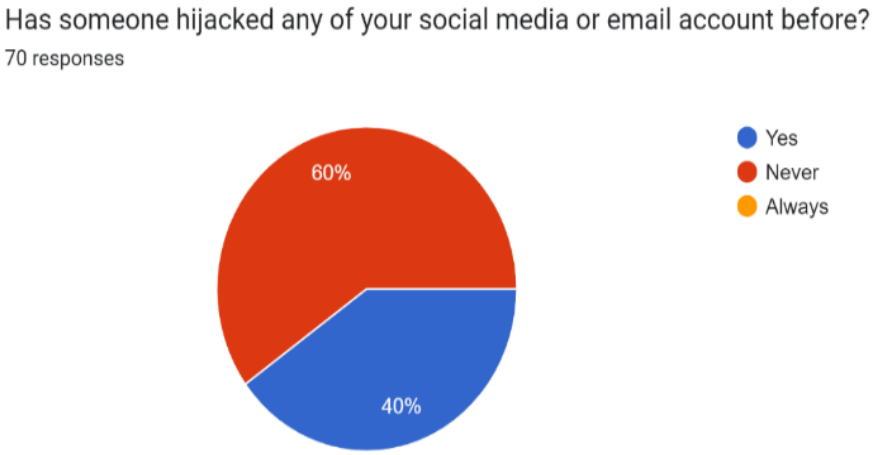



Figure 3. Incidence report from respondents.

Five-point rating scale was used to record, score of all positive statements which ranged from 5-1 for different response categories. Strongly agree (SA), Agree (A), Neutral (N), Disagree (DA) and Strongly Disagree (SDA). The data was analyzed in terms of percentage.

Some sample questions were taken from the questionnaire and analyzed. Table 1 examined the prevalent forms of cybercrime threats as rated by the respondents.

**Table 1.** Prevalent cyberthreats ratings.

| | Response | Level of agreement | | | | |
|---|---|---|---|---|---|---|
| Forms of cyberthreats | | SA | A | N | DA | SDA |
| Phishing | N | 28 | 30 | 12 | | |
| | % | 40 | 42.9 | 17.1 | | |
| Ransomware | N | 27 | 15 | 26 | 1 | 1 |
| | % | 38.6 | 21.4 | 37.1 | 1.4 | 1.4 |
| Software piracy | N | 22 | 41 | 7 | | |
| | % | 31.4 | 58.6 | 10 | | |
| Malware | N | 27 | 25 | 18 | | |
| | % | 38.6 | 35.7 | 25.7 | | |
| Cyberbullying | N | 26 | 39 | 4 | | 1 |
| | % | 37.1 | 55.7 | 5.7 | | 1.4 |
| Crypto jacking | N | 34 | 17 | 16 | 2 | 1 |
| | % | 48.6 | 24.3 | 22.9 | 2.9 | 1.4 |
| Credit card fraud | N | 24 | 37 | 8 | | 1 |
| | % | 34.3 | 52.9 | 11.4 | | 1.4 |

The respondents were exhaustive in the possible causes of increased cases of cybercrime in developing countries. It could be seen that poor implementation of cybersecurity laws, poor cybersecurity awareness, poverty and peer pressure were top on the list as shown in **Figure 4**.

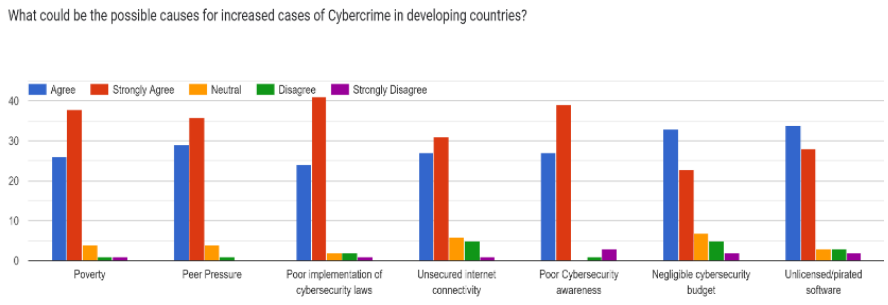



**Figure 4.** Causes of cybercrimes in developing.

The negative effects of cybercrimes were also listed out for respondents to asertain their levels of impacts. Identity theft, emotional distress, economic loss and loss of sensitive personal data were seen as the most negative impacts of cybercrimes as over 40 respondents from our sample population strongly concuured to the facts through their responses. Loss of life and reputational damage were considered as secondary negative effects as their impacts could not be compared at the same level as the afformentioned four negative impacts. Political instability had the most undecided votes as few wondered how cybercrimes could cause such a damage, nevertheless, 23 respondents strongly agreed that it is a negative effect

of cybercrimes. A more elaborate analysis is shown in Figure 5 below.

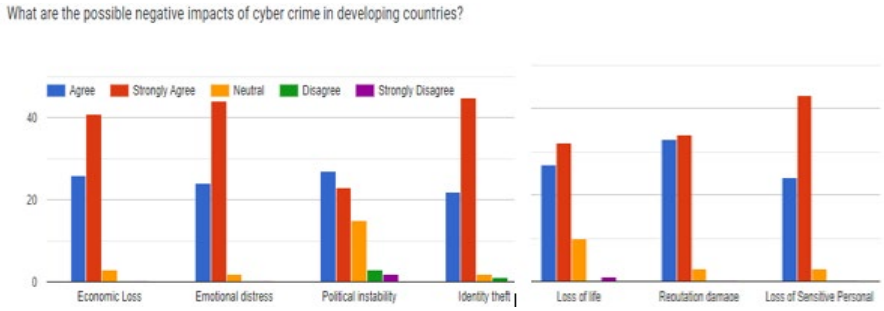



Figure 5. Negative impacts of cybercrimes in developing countries.

Compliance initiatives to cybersecurity measures was probed by this survey as well and Table 2 shows the summary of the findings rated in percentage.

The idea of having strong passwords with at least 12 variety of different breeds of characters is a very good policy. From the responses, it was seen that 47.1% complied fully whereas 41.4% were partial compliant and 11.4% were strictly non-compliant. In the compliance section of the survey, it was discovered that most individuals use same passwords for eternity without bothering to change it, only 14.3% of our sample size agreed that they regularly change their passwords at least every 90 days.

The use of Two-Factor Authentication (2FA) and Anti-Virus and Anti-Malware Software recorded a tremendous positive response in their usage as 71.4% and 67.1 respectively responded in affirmation to its usage, also there was 15.7% and 28.7% occasional compliance respectively leaving 12.9% and 3% as non-compliant individuals.

Encryption which is the Conversion of data into a code to prevent unauthorized access, using algorithms like AES (Advanced Encryption Standard) and RSA (Primary method of encrypting Data in Motion) is a secure way of transferring documents amongst users. From our survey, 22.9% did this always while 30% carried it out occasionally. A whopping 47.1% has never used such an important mechanism.

The Identification and remediation of vulnerabilities in software and systems appeared to be to be the Achilles heel of most respondents as 52.9% were disillusioned by it and only 21.4% carried it out sparingly. This left a paltry 25.7 respondents to be full compliant to this.

Regularly backing up critical data and having a plan in place to recover data in case of a loss is a standard that needs to be complied to. 67.1% responded in affirmation to the regular backup of data and 31.4% agreed that they do carry it out occasionally as only 1.4% never complied with such.

Protecting endpoints like laptops and smartphones with software and hardware controls is a very important measure but the feedback gotten showed that 34.3% do not have such mechanisms in place while 27.1% did such, occasionally? Only 38.6% considered such a measure important and ensured full compliance.

**Table 2.** Cybersecurity compliance measures.

| Cybesecurity measures | Responses in percentage (%) | | |
|---|---|---|---|
| | Affirmation | Occasionally | Never |
| Strong Password Policies (Minimum 12-character requirement) | 47.1 | 41.4 | 11.4 |
| Strong Password Policies (Periodic 90days Change) | 14.3 | 41.4 | 44.3 |
| Encryption | 22.9 | 30 | 47.1 |
| Two-Factor Authentication (2FA) | 71.4 | 15.7 | 12.9 |
| Anti-Virus and Anti-Malware Software | 67.1 | 28.6 | 3 |
| Vulnerability Management | 25.7 | 21.4 | 52.9 |
| Secure Backup | 67.1 | 31.4 | 1.4 |
| Secure Endpoint Protection | 38.6 | 27.1 | 34.3 |

It was also discovered that Incidence Response and Monitoring is actually a rare measure complied with by respondents. In cases of Cyber-attacks, only 27.1% of respondents had plans in place to respond, 51.4% had no plans at all and thus vulnerable. Only 21.4% had such mechanisms occasionally which is as good as not having it all because such attacks can happy at any time. Figure 6 summarized the responses.

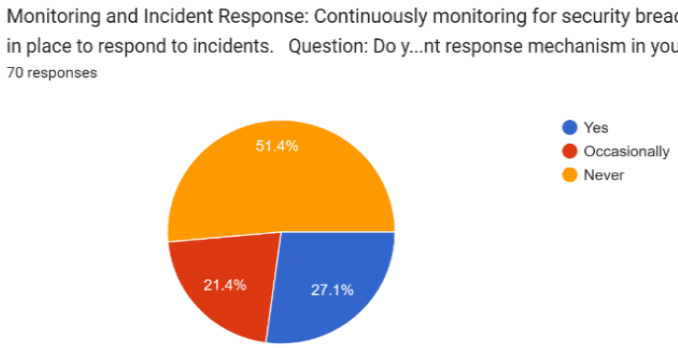



**Figure 6.** Incidence response plan from respondents.

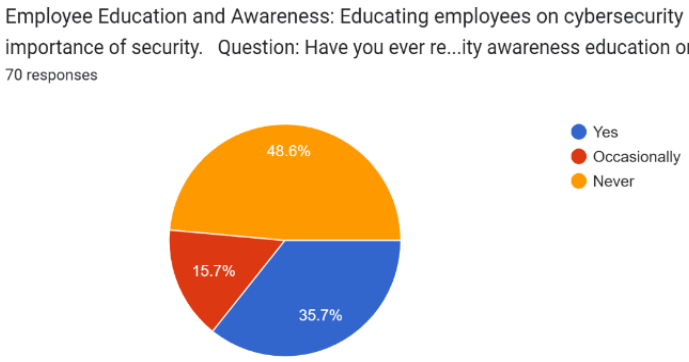



**Figure 7.** Cybersecurity awareness and orientation response from respondents.

The survey also explored the level of awareness and education gotten by individuals in their various places of work and businesses. 48.6% stated that they have never been enlightened on the various threats that exist in the cyber space and the measures to adopt to stay ahead of the attacks. Only 35.7% were in agreement that they have been educated about it while 15.7% stated that it only happened occasionally. This highlights that so much has to be done in cybercrime fight in developing countries. This is illustrated in Figure 7.

There was no good news as regards the continuous security assessment improvement which enables individuals to assess and stay ahead of threats. The responses left a lot to be desired of as shown in Figure 8. Half (50%) of the respondents does not have such measure in place.

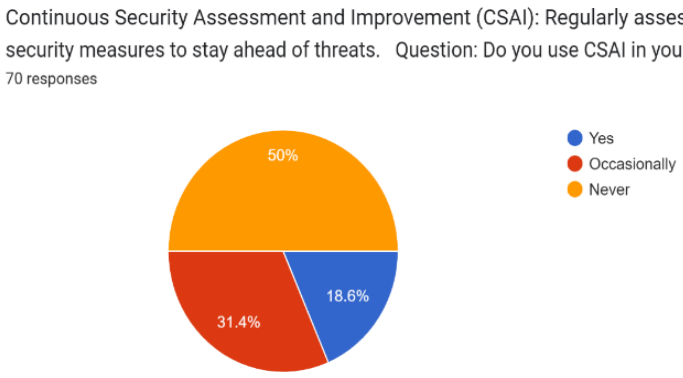



Figure 8. Continuous security assessment and improvement (CSAI) response from respondents.

Finally, it was discovered that there is no holistic hatred for cybercrime offenders and criminals as most respondents still had a soft spot for the crime and had no interest to fight against it as shown in Figure 9.

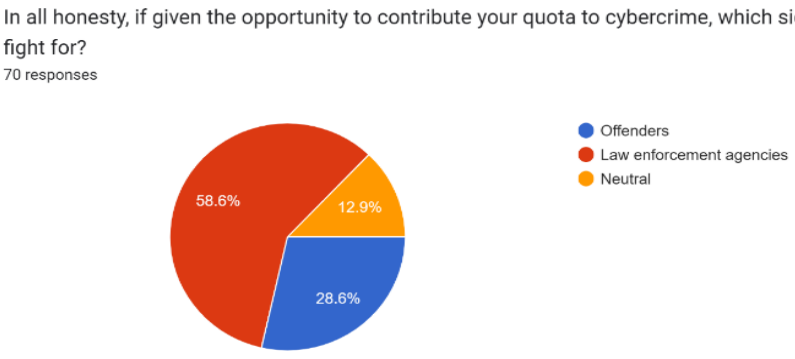



Figure 9. Response towards cybercrime offenders.

## 17. Discussion of Results and Findings

Cybercrime has been on a geometric rise in recent times in developing countries. This development has grown over the years unabated. The causes range from poverty to peer pressure, poor implementation of cybersecurity laws to lack of cyber-

security awareness, unlicensed and pirated software, to unsecured internet connectivity. According to [26], cybercrimes are committed in different forms. they include unauthorized access and hacking, web hijacking, pornography, child pornography, cyber stalking, denial of service attack, virus attacks, software piracy, salami attacks, phishing, sale of illegal articles, online gambling, email spoofing, cyber defamation, forgery, data diddling, etc. [28] categorized cybercrime thus:

(1) Crime against Individuals (a) Harassment via electronic mails (b) Dissemination of obscene material (c) Cyber-stalking (d) Defamation (e) Indecent exposure (f) Cheating (g)Unauthorized control/access over computer system (h) Email spoofing (i) Fraud.

(2) Crime against Individual Property (a) Computer vandalism (b) Transmitting virus (c) Unauthorized access/control over computer system (d) Intellectual Property crimes €Internet thefts.

(3) Crime against Organization (a)Unauthorized access/control over computer system (b)Cyber-terrorism against the government organization (c)Possession of unauthorized information (d)Distribution of Pirate software.

(4) Crime against Society (a) Child pornography (b) Indecent exposure of polluting the youth financial crimes (c) Sale of illegal articles (d) Trafficking (e) Forgery (f) Online gambling.

[29]-[31], and [32] state that the psychological effects of cybercrime are social withdrawal/anxiety, depression, PTSD, obsessive behaviors, loss of confidence, reduction in self-esteem, headaches, abdominal pain/stomach problems, eating disorder, sleep disorder, not feeling safe, self-harm, suicide tendencies, feeling helpless, panic attack, mistrust of others. [33] listed the following as critical negative repercussions cybercrime can inflict on businesses: **D**isruption of service or operations, financial repercussions, stolen or infringed intellectual property, forced changes in business practices, and reputational damage. [34] stated that while some cybercrime prevention strategies remain steadfast in warding off attackers, there is also been a new wave of modern technologies to help support these initiatives. These initiatives are advanced cybersecurity systems (like firewalls, antivirus software, and intrusion detection systems). Multifactor authentication, virtual private networks, email security solutions, password managers, security awareness training, data backup and recovery, and AI and ML cybercrime protection.

This research work was able to:

(1) Carry out an empirical analysis on the impact and panacea of cybercrime in developing countries.

(2) Deduce the major trending causes of cybercrime in developing counties and represent these causes using statistical tools.

(3) Deduce the major negative effects of cybercrimes on individuals, organizations, and states in developing countries.

(4) Make suggestions on the compliance of internet users in developing countries to cybersecurity standards.

Based on our findings from the empirical analysis, the following were agreed upon by the respondents as the major forms of cybercrimes in developing coun-

tries. They are Phishing, ransomware, software piracy, malware, cyberbullying, crypto jacking and credit card fraud.

Identity theft, emotional distress, economic loss and loss of sensitive personal data were seen from the responses of our respondents as the most negative impacts of cybercrimes. Loss of life, reputational damage and political instability were considered as secondary negative effects as their impacts could not be compared at the same level as the afformentioned four negative impacts.

Also, the following were agreed as the best measures to curb cybercrime in developing countries. These are strong password policy, encryption, two-factor authentication, anti-virus, anti-malware, vulnerability management, secure backup, and secure endpoint protection.

## 18. Conclusions

Developing countries have become a harbinger of cybercrimes and this development has grown over the years unabated. The causes of this growing menace which ranges from poverty to peer pressure, poor implementation of cybersecurity laws to lack of cybersecurity awareness, unlicensed and pirated software, to unsecured internet connectivity.

The growth of the internet has made imperative to curb this malaise. Judging from the analysis done on the compliance of users to some cybersecurity standards, it was discovered that users are not well educated on the dangers posed by using the internet and the various cybersecurity measures to adopt. Surprisingly, there was no holistic push towards joining the cybersecurity crusade to protect the internet space.

Hence, it could be seen that there are apologetics and enthusiasts on the proceeds of the negative effects of cybercrime thus making cybersecurity awareness a necessary panacea to be prioritized amongst others.

The internet is a fertile ground and lucrative space for all and sundry but the emergence of cybercrime is an enemy to its growth. The negative effects are enormous and thus causes ripple effects economically, politically, emotional and otherwise to individuals, organizations, governments and corporations in developing countries. This study is a clarion call for all especially Information Technology professionals to rise up to the occasion and nip the growth of this cancer worm at the bud through intensive and iterative cybersecurity awareness as well as implementation.

This study was a very significant Investigation as it contributed to knowledge in the following ways:

(1) Portrayed the extent this ugly malaise of cybercrime has eaten deep into the fabrics of developing countries.

(2) Discovery of a new level of digital divide which was as a result of non-compliance to cybersecurity ethics and standards.

(3) Establishment of the fact that software piracy is now a major cyber threat than most persons think.

It also reiterated the urgent need for cybersecurity awareness as the major key to effect compliance among individuals and professionals alike that have embraced the internet.

## Conflicts of Interest

The authors declare no conflicts of interest.

## References

[1] Interpol (2023) African Cyberthreat Assessment Report: Cyberthread Trends. United Kingdom-Foreign Commonwealth and Development Office (FCDO), Germany. https://www.cybilportal.org/

[2] World Economic Forum's Center for Cyber Security. https://www.weforum.org/agenda/2022/07/fraud-cybercrime-financial-business

[3] Kshetri, N. (2019) Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*, **22**, 77-81. https://doi.org/10.1080/1097198x.2019.1603527

[4] Adewopo, V., Sylvia, W.A., Mustapha, A.Y., Emmanuel, K.G., Ozer, M. and Elsayed, N. (2024) A Comprehensive Analytical Review on Cybercrime in West Africa. arXiv: 2402.01649.

[5] Iloanya, K.O., Eneh, M.I. and Ogechukwu, A.O. (2024) Effect of Cybercrime on the Academic Performance of Students of Tertiary Institutions in Enugu State, Nigeria. *Journal of Policy and Development Studies*, **15**, 126-144. https://doi.org/10.4314/jpds.v15i1.9

[6] Onyma, E.M., Ogechukwu, U. and Anthonia, E.C.D. (2019) Potentials of Mobile Technologies in Enhancing the Effectiveness of Inquiry-Based Learning Approach. *International Journal of Education* (*IJE*), **2**.

[7] Khan, A., Akram, S., Munir, S. and Almas, I. (2021) Causes and Effects of Cyber-Crime Victimization among Educated Youth: A Study of BZU, Multan. *IUB Journal of Social Sciences*, **3**, 40-45. https://doi.org/10.52461/ijoss.v3i2.829

[8] Akogwo, L.I. (2018) The Internet and Emergence of Yahoo-Boys Sub-Culture in Nigeria. *International Journal of Cyber Criminology*, **2**, 368-381.

[9] Adesina, O.S. (2017) Cybercrime and Poverty in Nigeria. *Canadian Social Science*, **13**, 19-29.

[10] Boateng, R., Olumide, L., Isabalija, R.S. and Budu, J. (2011) Sakawa-Cybercrime and Criminality in Ghana. *Journal of Information Technology Impact*, **11**, 85-100.

[11] Falowo, O.I., Popoola, S., Riep, J., Adewopo, V.A. and Koch, J. (2022) Threat Actors' Tenacity to Disrupt: Examination of Major Cybersecurity Incidents. *IEEE Access*, **10**, 134038-134051. https://doi.org/10.1109/access.2022.3231847

[12] Warner, J. (2011) Understanding Cyber-Crime in Ghana: A View from Below. *International Journal of Cyber Criminology*, **5**, 736.

[13] Panda Security (2023) Types of Cybercrime. https://www.pandasecurity.com

[14] Alexander, S.G. (2024) What Are Phishing Attacks? https://www.techtarget.com

[15] Tidmarsh, D. (2023) What Is Cybercrime? What Are the Different Types of Cyber Crime?

[16] CISCO (2024) What Is Malware? http://www.cisco.com

[17] (2003) Botnets, Cybercrimes and Cyberterrorism: Vulnerabilities and Policy Issues

for Congress. https://www.everycrsreport.com/reports/RL32114.html

[18] Dosal, B. (2023) Effects of Cybercrime for Business: The Hidden Cost. https://www.compuquip.com

[19] Stouuffer, C. (2024) Cyberstalking: What It Is and How to Protect Yourself. https://us.norton.com

[20] Soltan, F. (2024) The Hidden Impact of Cyber Attacks on Mental Health. https://acronymsolutions.com

[21] Kosinski, M. (2024) What Is Data Breach? https://www.ibm.com

[22] Kshetri, N. (2013) Cybercrime and Cybersecurity in the Global South. Palgrave Macmillan.

[23] Kshetri, N. (2015) Cybercrime and Cybersecurity Issues in the BRICS Economies. *Journal of Global Information Technology Management*, **18**, 245-249. https://doi.org/10.1080/1097198x.2015.1108093

[24] Shea, S. and Alexander, S.G. (2024) Cybersecurity. https://www.techtarget.com

[25] WaterISAC (2016) 10 Basic Cybersecurity Measures: Best Practices to Reduce Exploitable Weaknesses and Attacks. https://www.waterisac.org

[26] Indian Cyber Squad (2024) Cyber Crime Types. https://www.indiancybersquad.org/cyber-crime-types

[27] Anwita (2024) 15 Best Cybersecurity Tools in 2024. https://www.sprinto.com

[28] Christopher, U.E., Samuel, O.J.O., Chioma, A. and Edward, A.G.U. (2020) Cybercrime, Its Adherent Negative Effects on Nigerian Youths and the Society at Large: Possible Solutions. *International Journal of Advances in Scientific Research and Engineering*, **5**, 155-164. https://doi.org/10.31695/ijasre.2019.33658

[29] Bates, S. (2016) Revenge Porn and Mental Health: A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors. *Feminist Criminology*, **12**, 22-42. https://doi.org/10.1177/1557085116654565

[30] Låftman, S.B., Modin, B. and Östberg, V. (2013) Cyberbullying and Subjective Health: A Large-Scale Study of Students in Stockholm, Sweden. *Children and Youth Services Review*, **35**, 112-119. https://doi.org/10.1016/j.childyouth.2012.10.020

[31] Schneider, S.K., O'Donnell, L., Stueve, A. and Coulter, R.W.S. (2012) Cyberbullying, School Bullying, and Psychological Distress: A Regional Census of High School Students. *American Journal of Public Health*, **102**, 171-177. https://doi.org/10.2105/ajph.2011.300308

[32] Sourander, A., Brunstein Klomek, A., Ikonen, M., Lindroos, J., Luntamo, T., Koskelainen, M., *et al.* (2010) Psychosocial Risk Factors Associated with Cyberbullying among Adolescents: A Population-Based Study. *Archives of General Psychiatry*, **67**, 720. https://doi.org/10.1001/archgenpsychiatry.2010.79

[33] Joanne, G. (2023) What Are the Negative Effects of Cyber Crime? https://www.sigmadrm.com/blog/detail?slug=what-are-the-negative-effects-of-cyber-crime

[34] Proofpoint (2024) What Is Cybercrime? https://www.proofpoint.com/us/threat-reference/cyber-crime