**A Design Brief**

**The Problem Statement:** How might we mitigate the rate of youth’s engagement in cybercrime in Nigeria?

**What is Cybercrime?**

**Cybercrime** refers to any criminal activity that are carried out by means of computer or the internet.

These activities target the security of computer systems or networks.

**The Refined Problem Statement:** How might we improve the youth’s socio-economic independence and ensure that cyber criminals are prosecuted?

**Design Strategy Statement:** Our project is to build an online platform dedicated to the youths which will provide socio-economic development opportunities and fight cybercrime, specifically in the Nigerian context.

**Understand Phase**

The methods that were employed in the Understand Phase to perform a context review on the problem statement were:

* Desk Research
* Expert Interview

**The Desk Research**

While conducting our desk research, we came up with following research questions and sourced for answers from online articles and texts from various authors:

1. **Why do we have this problem?**

* Why is cybercrime rampant in Nigeria?
* Why are the youths engaging in cybercrime in Nigeria?

1. **Poverty and economic inequality** Many people are struggling to make ends meet due to limited job opportunities and increasing hardship in Nigeria. This implies that Nigeria struggles with wealth inequality. Many individuals therefore see cybercrime as a means to address this imbalance by obtaining illegal wealth, as they are frustrated. Many people who engage in cybercrime get rich quick and this perception motivates people to engage in cybercrime activities.

1. **High rate of unemployment**

Nigeria has a large youth population with limited job opportunities. According to a research done by Hassan in 2012, it is known that over 20 million graduates in Nigeria do not have gainful employment. Many young people therefore turn to cybercrime as a way to make quick money as it can offer significant financial rewards when compared to traditional employment (which is not even available).

1. **Lack of awareness**

Most youths are not aware of the risks and consequences associated with cybercrimes.

On the other hand, the public is not aware of existing or emerging trends in cybercrime as there is no central hub or platform where information on cybercrime can be documented and publicized.

Lots of cybercrime activities go unreported as the victims often times do not have the right platform to channel their complaints and the few who get to report do not get closure as the perpetrators are not brought to justice.

1. **Low risk perception**

The perception of low risk and weak law enforcement encourages cyber criminals to engage in illegal activities knowing that there are little to no consequences associated.

1. **Weak cybercrime law enforcement/legal framework**

Nigeria’s law enforcement is weak and severely underfunded. Cybercrime laws in Nigeria are therefore historically less robust compared to other countries. This has allowed cyber criminals to operate with relative impunity, as the legal framework is not equipped enough to address emerging cyber threats effectively.

1. **Large population**

Nigeria has a population of over 200 million people with many of them young and tech savvy. This large pool of potential victims makes Nigeria a lucrative target for people that carry out cybercrime.

1. **Global collaboration**

Cyber criminals in Nigeria often collaborate with counterparts from around the world. These international networks can be difficult to track and dismantle, making it challenging for law enforcement agencies to apprehend cybercriminals.

1. **Cultural factors/peer pressure**

There is a common perception that engaging in cybercrime can be a form of ‘get rich quick’ entrepreneurship, especially in an environment where conventional opportunities are limited and high levels of illiteracy in Nigeria.

1. **Who are we solving the problem for?**

* What set of people stand to benefit if cybercrime is reduced in Nigeria?
* What set of people does cybercrime affect more in Nigeria?

1. **Nigerian youths (12 – 50 years)**

Anyone with a mobile phone in their pocket, anyone who has a bank account, anyone who stores important files on their computer, anyone whose name is in a direct marketing database, anyone with an ATM card

1. **Internet Users**

Anyone who uses the internet can be vulnerable to cybercrimes such as phishing, identity theft, online scams, and malware attacks.

1. **Elderly Population**

Older individuals may be less familiar with technology and more susceptible to various online scams and frauds.

1. **Businesses**

Small and Medium-Sized Enterprises (SMEs): SMEs are often targeted by cybercriminals due to potentially weaker cyber security measures compared to larger corporations.

Large Corporations: Major corporations can also fall victim to cyber attacks, which may result in data breaches, financial losses, and reputational damage.

1. **Children and Adolescents**

Children and teenagers are vulnerable to cyberbullying, online harassment, and exposure to inappropriate content. Young individuals may be targeted by online predators, posing risks to their safety.

1. **Minority and Vulnerable Groups**

Certain groups, such as racial or ethnic minorities, may be targeted for hate speech, discrimination, or online harassment.

1. **Journalists and Activists**

Cyber attacks on journalists can infringe on press freedom and hinder investigative reporting. Activists may also face online harassment, hacking attempts, and surveillance from adversaries.

1. **The Nigerian economy**

The Nigeria economy including the enormous amount of e-business are greatly threatened by the rapid increase of cybercrimes. In a 2016 article by This Day and Vanguard, Senator Iroegbu estimated the annual cost of cybercrimes to Nigeria at about 0.08% of the GDP, which amounts to 127billion.

1. **What is the goal or objectives for solving this problem?**

* What does Nigeria stand to gain if cybercrime is reduced?
* Why should we strive to reduce youths engagement in cybercrime in Nigeria?

1. **Improved public image**

Nigeria is ranked third amongst the top ten sources of cybercrime in the world behind the US by 8% (65%) and the UK (9.9%). Furthermore, Nigeria is ranked first in the African region as the focus and root of malicious cyber activities, according to Ribadu (2007), and this is spreading across the West African sub-region.

A cyber security expert was once asked to describe how other countries see Nigeria when it comes to cybersecurity and he replied, “can anything cyber-good ever come out of Nigeria?” (Ifeoma Okeke-Korieocha 2023).

Reducing cybercrime in Nigeria will correct the bad impression that other countries have about us.

1. **Improved opportunities for Nigerians**

According to Abimbola (2013), cybercrime impedes the country’s socioeconomic growth because it fosters a lack of trust and faith in profitable transactions, encourages the denial of innocent Nigerians opportunities abroad, and results in job losses and revenue loss. According to Greener Journal of Social Sciences, Vol. 13(1), pp. 4-9, 2023, beside the implications of being tagged a cybercrime enabling nation, the country and its citizens stand to lose both tangible and intangible resources within and outside the country.

Tackling cybercrime will restore trust in the country’s digital infrastructure and citizens and this will in turn lead to boost in foreign investments and international trades.

1. **Improved socio-economic growth**

According to the findings of Maitanmi et al (2013) due to the low level of trust cybercrimes has generated in the Nigerian economy, cybercrime impedes Nigeria’s socio-economic growth by driving away foreign investors. Therefore mitigating youths engagement in cybercrime will improve socio-economic growth.

1. **Reduced economic loss**

Our society loses millions of naira due to cybercrime perpetrators. Reducing cybercrime will boost the country’s economy and workplace which will lead to economic growth and development. According to NCC, Nigeria loses about 500m dollars yearly to cybercrime, which accounts for 0.08% of the GDP.

1. **National security**

protecting critical infrastructure and data protects national security interests.

1. To help reduce the vulnerability of information and communication technology systems and networks.
2. To boost moral positivity and impact productivity in the work place
3. To help industries and organizations develop and nurture a culture of cybersecurity that will lead to a more secured cyberspace.
4. **With what are we going to solve the problem?**

* What materials or resources do we need to use to tackle cybercrime in Nigeria?
* What resources can we use to create opportunities for the youths and raise awareness about the consequences of cybercrime in Nigeria?

1. Provision of more skilled cybersecurity professionals and funding for cybersecurity initiatives to keep up with latest technology and best practices to combat cybercrime.
2. Increased investment in cybersecurity and creating of a functional online platform to document and track cybercrime. Youths can also register on the platform to acquire skills and also apply for advertised job opportunities that will boost their financial independence.
3. Providing cybersecurity training and education to employees/individuals on the identification and prevention of cybercrime.
4. Creating laws and regulations to combat cybercrime, and training cyber police to enforce these laws.
5. Robust cybersecurity plan that includes regular security assessment and checks, checks of witnesses in systems, incident reports, response and disaster recovery procedures to minimize the impact of a succesful cyber attack, implementation of advanced security technology such as firewalls, intrusion detection, prevention systems and multifactor authentication to protect systems.
6. Subsidizing cybersecurity education and training programs in the country. Creating avenues for youths to be gainfully engaged in activities that will bring about socioeconomic independence.
7. International co-operation: According to Nayak (2018), governments and industries have gradually realized the colossal threats of cybercrime on economic/political security and public interests. However, complexity in types of cybercrime calls for international cooperation. Sequel to this, various organizations and governments have already made joint efforts in establishing global standards of legislation and law enforcement both on a regional and on international scale. U.S.-China`s cooperation is one of the most striking progress recently because they are the top two source countries of cybercrime (Nayak, 2018). Thus, Agbu (2019) stated that due to the heterogeneity of law enforcement and technical counter measures of different countries, there is need for legislative and regulatory initiatives of international cooperation to control or curb the activities of cyber criminals. Though law enforcement agencies are trying to tackle this problem, it is growing regularly and many people have become victims of identity theft, hacking and malicious software. Therefore, one of the best ways to stop these criminals and protect sensitive information is by making use of inscrutable security that uses a unified system of software and hardware to authenticate any information that is accessed over the internet.
8. **Who else is solving the problem?**

* Are their bodies or establishments in Nigeria that are tackling cybercrime?
* Are their international bodies that might be willing to collaborate with Nigeria to fight cybercrime and provide job opportunities for Nigerian youths?

1. The Nigeria Police Force Cybercrime Unit established in 2017
2. Nigeria Cyber Crime Working Group NCCWG
3. Internet Crime Complaints Center (IC^3) established in May 2000 by the Federal Bureau of Investigations FBI
4. Economic and Financial Crimes Commission (EFCC).
5. National Information and Technology Development Agency (NITDA)
6. **How much do you think it will cost to reduce cybercrime in Nigeria?**

The cost of reducing cybercrime in Nigeria can vary widely depending on the scope of the efforts, the specific strategies, initiatives involved and the duration of the cyber security programs that are put in place.

Tackling cybercrime is a complex and ongoing endeavor that requires investments in various areas. These investments can run into several billions of Naira.

A 2018 African cybersecurity study says that Nigeria spent an estimated sum of $270.22 million to prevent cyberattacks.

In 2021 budget, the entire security sector allocation was 1.97 trillion naira

Research firm, Gartner Inc. estimates that cybersecurity spending in Nigeria in 2021 totaled about $150 billion, up more than 12% from 2020. Spending in 2022 is likely to continue to grow rapidly, as the number of threats, as well as cybersecurity solutions and their costs increase.

Other restrictions that may hinder reduction of cybercrime in Nigeria include corruption and non-government participation.

1. **When do you think cybercrime will be reduced in Nigeria, if the different measures are put in place?**

**For the first twelve months**, the team will go out into the field to observe the people in their communities, gather all relevant information on cybercrime and cybersecurity, and document every finding.

**For the next two and half years**, this will involve employing all members of the online development team (e.g. product designers, software developers, product managers, QA testers, etc.), coming up with user stories, creating product roadmaps etc. and eventually building the online platform.

**For the next twelve months**, the marketing team will start sensitizing the public (especially the youths) about the online platform, getting them to register on the platform, to apply to acquire tech skills advertised on the platform, and getting them to be job ready in the tech industry.

**In the next one year**, we should already have youths getting job roles on the platform. The public awareness is full blown, and virtually every youth is aware of the dangers of engaging in cybercrime. They will also know that they can register to acquire skills on the platform and get job placements after completing their program.

**Basically, in five and half years a visible reduction in cybercrime should be in effect.**

1. **How? – Next Steps**

* How can we harness the power of technology to create innovative solutions and platforms that will discourage youths from engaging in cybercrime in Nigeria?
* What is the way forward for the Nigerian youths after we have discouraged them from engaging in cybercrime.
* What kind of opportunity can we create to further prevent youths from engaging in cybercrime in Nigeria?

1. We plan to build an online platform that will offer comprehensive training programs at subsidized rates in digital skills (programming, cybersecurity, e.t.c.) to all youths in Nigeria.

These programs will ensure that the youths acquire the required skills to excel in the tech industry; this is essential because the youths that engage in cybercrime already have interest in technology.

1. The platform will also offer job placements for the youths upon completion of their trainings. (Companies and organizations will be able to advertise vacant roles on the platform).
2. The online platform will also create awareness to everyone; especially the youths on the dangers of engaging in cybercrime. Proper and adequate sensitization should be given to every person at various levels to ensure that they become smart and guide themselves against the criminals who try to steal their joy via the internet.
3. Cyber criminals when caught should be publicly prosecuted to serve as a deterrent to other youths that may want to engage in cybercrime.
4. Children supervision

When children use the internet, they should be adequately supervised. They shouldn’t be allowed to visit just any site. Ideally, before parents hand an internet-enabled device to a child, the device should have some software pre-installed in it that avoids a visit to some websites prone to Cybercrimes.

1. Some information like the one displayed below showed be put up on the platform to further sensitize the public:

It begins with you also.

It is not enough to be protected by government agencies, individuals should also protect themselves.

Your passwords should be strong and reserved for you alone

Say less to strangers on social media handles and websites.

The less a person you do not know personally knows about you, the safer you are.

Cybercriminals only work with the information they have; If you give them nothing, they know nothing and they’ll do you nothing.

**The Expert Interview**

**Interviewee**: E. Swanson

**Sex:** Male

**Age bracket**: Early 20s (20-25)

**Ethnicity**: Yoruba tribe

**Nationality**: Nigerian

**Profession:** Cybersecurity expert

**Years of experience**: 1.5 years

Currently working in the UK.

**Why?**

People engage in cybercrime majorly because they are trying to escape poverty. They feel like going through the legal means is slow and most times ends up not being beneficial. Other reasons include greed, curiousity (script kiddies) etc.

There is also family/societal pressure to make money and provide for the family.

**Who?**

Anyone can be a victim of cybercrime, but the people who are more susceptible include older people who are not really familiar with technological advancement and require help. They end up falling for phishing scams. Young kids or youth are also susceptible as they are just navigating life.

**What?**

Improved public image: Nigerians are notorious for cyber crime in the international community. Therefore, if cybercrime is reduced, this will improve our international image.

Lesser lost opportunities: Nigerians are intelligent people with alot to offer. Our human capital is valuable to other countries. If cybercrime is reduced, international companies will have more trust in employing Nigerians.

**With What?**

Awareness on cybercrime and its consequences can be created through the use of social media and mainstream media such as bill boards and TV, walks and talks to public places such as schools, to educate people on the importance of safeguarding personal information.

More effort should also be put into creating awareness for people at risk of cybercrime, and creating more job opportunities.

**Who Else?**

The Economic and Financial Crimes Commission.

Department of State Services (DSS) handle cybercrimes of national importance.

However, most government bodies meant to tackle cybercrimes are compromised already.

Most international bodies that can help cannot collaborate with us because of our notoriety for cybercrimes. Some of these bodies may also need to be formally invited by the Nigerian government.

**How Much?**

Billions of naira.

This is because of all the measures you would need to put in place to not just tackle cybercrime, but to also create awareness, create jobs and other opportunities for people to learn skills that they can use to do better in life.

**When?**

A very long time. This is because even some law makers are engaging in cybercrime as well, so the change has to start from everyone at the grassroot. We would also need to solve all the problems/reasons that make people go into cybercrime in the first place.

**How?**

Nigerians enjoy challenges that involve financial compensation. If the government can put up a financial incentive to divert people’s attention from cybercrime to other alternatives like learning new skills, the rate of cybercrime in Nigeria will reduce.

The government should work on creating NGOs to specialize in reforming cyber criminals.

Interested foreign investors can also come in to invest and train Nigerians on more useful skills.

Other things that can be done include creating more employment opportunities.

Awareness of cybercrime and its dangers should also be taught at lower ages in schools.

Youth and their families should be educated on the dignity of labor and how parents need to reduce pressure on children to make money for the family.