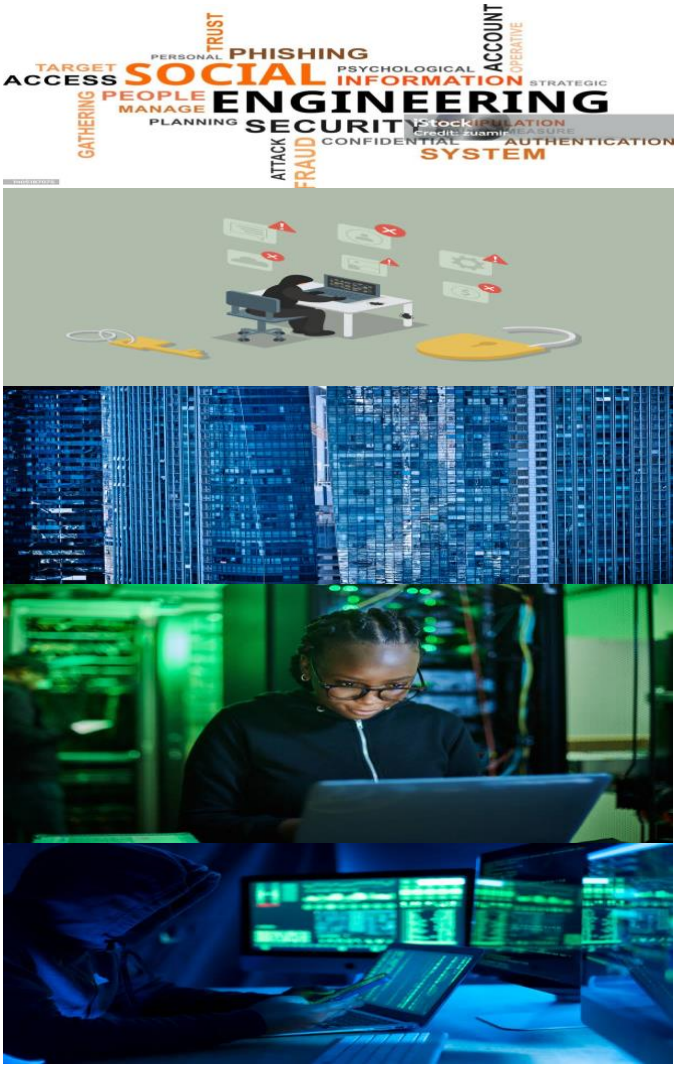


SOCIAL ENGINEERING AND A STRONG/ENFORCEABLE LEGAL FRAMEWORK: A PATH TO ACCOUNTABILITY

BY:
CHINELO AUDREY OFOEGBUNAM
+234(0)7036115290, +234(0)8027120428
ciaofoegbunam@gmail.com
December 12, 2024

ABSTRACT

The proliferation of social engineering attacks in Nigeria has underscored the need for a robust and enforceable legal framework to combat this menace. This paper examines the intersection of social engineering and the legal framework in Nigeria, highlighting the challenges and gaps in existing laws and regulations. It argues that a strong and enforceable legal framework is essential for holding perpetrators accountable and providing remedies for victims. We employed the mixed-methods approach, combining both qualitative and quantitative methods to collect and analyze data using the literature review, surveys, interviews, and case study with thematic and content analysis, descriptive statistic and ethical considerations with limits to Nigeria. The paper proposes a path to accountability, which includes the development of specialized courts and tribunals, updating laws and regulations, promoting public awareness, and fostering international cooperation. Ultimately, this paper seeks to contribute to the discourse on social engineering and the law in Nigeria, with a view to promoting a safer and more secure online environment.

TABLE OF CONTENTS

1. Introduction ---------- 3
1.1 Background
1.2 Problem Statement
1.3 Research Questions
1.4 Objectives
1.5 Scope

2. Social Engineering in Nigeria: An Overview ---------- 4
2.1 Prevalence of Social Engineering
2.2 Types of Social Engineering Attacks
2.3 Impact of Social Engineering on Individuals and Organizations

3. Legal Framework for Social Engineering in Nigeria ---------- 6
3.1 Cybercrime (Prohibition, Prevention, etc.) Act 2015
3.2 Advance Fee Fraud and Other Related Offences Act 2006
3.3 Other Relevant Laws and Regulations

4. Challenges in Combating Social Engineering in Nigeria ---------- 11
4.1 Technical Challenges
4.2 Legal Challenges
4.3 Institutional Challenges

5. A Path to Accountability: Recommendations ---------- 13
5.1 Development of Specialized Courts and Tribunals
5.2 Updating Laws and Regulations
5.3 Promoting Public Awareness
5.4 Fostering International Cooperation

6. Conclusion ---------- 15
6.1 Summary of Findings
6.2 Implications for Policy and Practice
6.3 Future Research Directions

7. References ---------- 17

"Social Engineering and a Strong/Enforceable Legal Framework: A Path to Accountability" at The Continuing Legal Education Committee Program for the Nigerian Bar Association, Degama Branch Law Week, 2024, Port Harcourt, Nigeria.

Paper Presenter: Chinelo Audrey Ofoegbunam.

The internet and digital technologies have transformed the way we live, work, and interact with one another. However, this growth has also created new opportunities for malicious actors to exploit vulnerabilities and commit crimes. One of the most significant threats in this regard is social engineering, which involves the use of psychological manipulation to deceive individuals into divulging sensitive information or performing certain actions that compromise security.

I. INTRODUCTION

The rapid advancement of technology has brought about unprecedented opportunities for social interaction, communication, and innovation. However, this digital age has also given rise to new challenges, particularly in the realm of social engineering. Social engineering refers to the manipulation of individuals into divulging confidential information or performing certain actions that compromise security. As technology continues to evolve, social engineering tactics are becoming increasingly sophisticated, making it imperative to develop a robust legal framework to combat these threats.

In Nigeria, social engineering has become a significant concern, with many individuals and organizations falling victim to various types of social engineering attacks. These attacks can have devastating consequences, including financial loss, reputational damage, and compromised national security.

Despite the growing threat of social engineering, Nigeria's legal framework for combating this menace is still evolving. While there are some laws and regulations in place, such as Cybercrime (Prohibition, Prevention, etc.) Act 2015, there is a need for a more comprehensive and enforceable legal framework to hold perpetrators accountable and provide remedies for victims.

This presentation seeks to contribute to the discourse on social engineering and the law in Nigeria. It examines the concept of social engineering, its impact on individuals and organizations, and the current legal framework for combating social engineering in Nigeria. The paper also identifies the challenges in combating social engineering and proposes a path to accountability, including the development of specialized courts and tribunals, updating laws and regulations, promoting public awareness, and fostering international cooperation.

Ultimately, this paper aims to provide a comprehensive analysis of the intersection of social engineering and the law in Nigeria, with a view to promoting a safer and more secure online environment.

II. UNDERSTANDING SOCIAL ENGINEERING

Social engineering is a growing concern globally, and Nigeria is no exception. It is the use of psychological manipulation to deceive individuals into divulging sensitive information or performing certain actions that compromise security[1]. It is the art of manipulating or gaining unauthorized access to systems, networks, or physical spaces. Thus, it is a non-technical attack that exploits human psychology, trust, and behavior.

Social engineering is a significant threat to individuals and organizations in Nigeria. These attacks are increasingly common in Nigeria. According to a survey by the Nigerian Communications Commission (NCC), 71% of respondents reported experiencing social engineering attacks in 2020[2]. Another study found that 45% of Nigerian organizations experienced social engineering attacks in 2019[3].

Types of Social Engineering[4]

There are several types of social engineering attacks, including phishing, pretexting, baiting, quid pro quo, etc.

1. Phishing: This attack involves sending or using fraudulent emails, messages, or phone calls to trick victims into revealing sensitive information.
2. Pretexting: Creating a false scenario to gain trust and obtain information.
3. Baiting: Leaving malware-infected devices or storage media in public areas to entice victims.
4. Quid Pro Quo: Offering a benefit or service in exchange for sensitive information.
5. Tailgating: Following authorized personnel into secure areas.
6. Whaling: Targeting high-level executives or officials with sophisticated phishing attacks.
7. Vishing: Using voice calls to trick victims into divulging information.
8. Smishing: Sending text messages to trick victims into divulging information.

Impact of Social Engineering

---

[1] Hadnagy, C. (2010). Social engineering: The art of human hacking. Wiley Publishing.

[2] NCC. (2020). 2020 Cybersecurity Threats and Trends Report.

[3] KPMG. (2019). Cyber Security Survey Report.

[4] Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and Applications, 20, 44-54.

Social engineering attacks can have devastating consequences, including financial loss, reputational damage, compromised national security[5], and even cause psychological trauma for victims. In Nigeria, social engineering attacks have resulted in significant financial losses for individuals and organizations[6].

Social Engineering Tactics:
1. Authority: Impersonating a figure of authority to gain trust.
2. Urgency: Creating a sense of urgency to prompt action.
3. Scarcity: Creating a sense of scarcity to prompt action.
4. Reciprocity: Offering a benefit or service to gain trust.
5. Commitment and Consistency: Encouraging victims to commit to a decision or action.

Protecting ourselves and our organization:
1. Awareness: Educate oneself and others about social engineering tactics.
2. Verification: Verify the identity of individuals and organizations before divulging information.
3. Policies: Establish and enforce strict security policies and procedures.
4. Training: Provide regular training to train, and retrain on social engineering tactics and best practices.
5. Incident Response: Establish an incident response plan to respond to social engineering attacks.

The Nigerian Context
Nigeria, with its growing digital landscape, is particularly vulnerable to social engineering attacks. The country's increasing reliance on technology for financial transactions, communication, and data storage creates an attractive target for cybercriminals. Moreover, the lack of a comprehensive legal framework to address social engineering has created a culture of impunity, allowing perpetrators to act with relative ease.

Real-World Examples:
1. The Prince Scam: A classic phishing scam where victims are promised a large sum of money in exchange for their bank account details.
2. The Target Data Breach: Hackers used social engineering tactics to gain access to Target's systems, resulting in a massive data breach.

---

[5] Abawajy, J. (2014). User preference of cyber security measures to protect online transactions. International Journal of Electronic Commerce, 18(2), 159-186.
[6] CBN (2020). Cybersecurity threats and risks in the Nigerian financial sector. Central Bank of Nigeria.

3. The Google and Facebook Scam: Scammers used social engineering tactics to trick Google and Facebook into transferring $123 million to their bank accounts.

Gap in Literature

While there is a growing body of literature on social engineering, there is a need for more research on the specific challenges and opportunities for combating social engineering in Nigeria.

III. THE NEED FOR A STRONG LEGAL FRAMEWORK

A strong and enforceable legal framework is essential in combating social engineering. Such a framework should provide clear guidelines on the responsibilities of individuals, organizations, and government agencies in preventing and responding to social engineering attacks.

Key components of this framework should include:

1. Definition and Classification of Social Engineering: A clear definition of social engineering and its various forms should be established to facilitate identification and prosecution.
2. Regulation of Data Protection: Stringent data protection regulations should be enacted to ensure that organizations handling sensitive information implement adequate security measures to prevent unauthorized access.
3. Establishment of Cybercrime Units: Specialized cybercrime units should be established within law enforcement agencies to investigate and prosecute social engineering cases. E.g., EFCC, DSS, etc.
4. Public Awareness and Education: Public awareness campaigns should be launched to educate individuals on the dangers of social engineering and how to protect themselves.
5. Develop specialized courts and tribunals: Establish specialized courts and tribunals to handle social engineering cases and provide specialized training for judges and law enforcement agencies.
6. Develop incident response plans: Develop incident response plans to quickly respond to social engineering attacks and minimize damage.

Legal Framework for Social Engineering

The legal framework for combating social engineering in Nigeria is still evolving. The Cybercrime (Prohibition, Prevention, etc.) Act 2015 is the primary legislation addressing cybercrime, including social engineering[7]. However, the law has been

[7] NCC (2015). Cybercrime (Prohibition, Prevention, etc.) Act 2015. Nigerian Communications Commission.

criticized for being inadequate and not providing sufficient penalties for perpetrators[8].
The legal framework for social engineering in Nigeria refers to the laws, regulations, and policies that govern and regulate social engineering activities in Nigeria.

In essence, it encompasses the following:
1. Laws: Statutes, acts, and decrees that prohibit and punish social engineering activities, such as phishing, advance fee fraud, and identity theft.
2. Regulations: Rules and guidelines issued by regulatory bodies, such as the Nigerian Communications Commission (NCC), Central Bank of Nigeria (CBN), and Economic and Financial Crimes Commission (EFCC), to prevent and combat social engineering.
3. Policies: Guidelines and procedures established by organizations, institutions, and government agencies to prevent and respond to social engineering attacks.
4. Enforcement mechanisms: Institutions and agencies responsible for enforcing laws and regulations related to social engineering, such as the EFCC, Nigeria Police Force, and courts.

The legal framework for social engineering in Nigeria **aims** to:
1. Prevent social engineering activities
2. Protect individuals and organizations from social engineering attacks
3. Punish perpetrators of social engineering crimes
4. Promote cybersecurity and online safety[9]

International Best Practices

Several countries have implemented robust legal frameworks and strategies to combat social engineering. For example, the United States has the Computer Fraud and Abuse Act (CFAA), which provides severe penalties for computer-related crimes, including social engineering[10]. Similarly, the European Union's General Data Protection Regulation (GDPR) provides a comprehensive framework for protecting personal data and combating social engineering[11].

Technology and Law Integration in Nigeria

Some of the key laws and regulations that form part of the legal framework for social engineering in Nigeria include:

---

[8] Adeyemo, D. (2017). Cybercrime and cybersecurity in Nigeria: An appraisal of the Cybercrime (Prohibition, Prevention, etc.) Act 2015. Journal of Cybersecurity, 3(1), 1-12.
[9] Cybercrime in Nigeria: Challenges and Prospects" by the Nigerian Institute of Advanced Legal Studies (2019)
[10] USDOJ (2020). Computer Fraud and Abuse Act. United States Department of Justice.
[11] EU (2016). General Data Protection Regulation. European Union.

Court Rules and Practice Directions

1. Federal High Court (Civil Procedure) Rules 2009: Provides guidelines for electronic filing and service of court processes, which can be used to combat social engineering. See, **Enukora v. F.R.N (2018) LPELR-43822(SC).**

2. **High Court of Lagos State (Civil Procedure) Rules 2024**: Provides guidelines for electronic filing and service of court processes, which can be used to combat social engineering.

Laws and Judicial Decisions:

1. **Cybercrime (Prohibition, Prevention, etc.) Act (2015):** This is the primary legislation addressing cybercrime in Nigeria. The Act prohibits and punishes various types of cybercrimes, including social engineering. Specifically, Section 32 of the Act makes it an offense to use a computer system or network to commit social engineering. Thus, it prohibits and punishes cybercrime. For example; Section 24[12] Prohibits and punishes phishing, which is a type of social engineering.

In **Adekola v. F.R.N**.[13] the Court of Appeal Per (**Umar J.C.A**), rightly held;

> ***"The court would not hastily interfere with the statutory powers of law enforcement agencies in the exercise of their statutory right to investigate alleged offences and detain, where necessary, for purposes of that investigation. The attitude of the courts is to deal with each case of arrest and detention on its merits when it occurs and comes before them. [Danfulani v. EFCC (2016) 1 NWLR (Pt. 1493) 223; Kalu v. F.R.N. (2016) 1 NWLR (Pt. 1516) 1 referred to.] (P. 242, paras. B-D)"***
>
> And
>
> ***"The penalty provided in section 22(2) of the Cybercrime (Prohibition, Prevention, E.t.c.) Act 2015, on which the appellant was tried and convicted is an imprisonment for a term of 5 years or a fine of not more than N7,000,000 or both. But the appellant was sentenced to a term of two and a half year imprisonment, which is a punishment lesser than the maximum sentence prescribed in the law."***

And in **Dawan v. E.F.C.C**.[14] Per (**Ugo J.C.A)** held;

> ***"In his judgment, the lower court (Kurya, J.) held that: From the process filed 8th respondent had 'clearly shown' that appellant was***

[12] Cybercrime (Prohibition, Prevention, etc.) Act (2015)

[13] (2024) 10 NWLR (Pt. 1946) 297 at 309, paras. F-G

[14] (2020) 5 NWLR (Pt. 1717) 226

involved in monumental (1) International Cybercrime. That 'the staggering sum of N908,271.096.00 is the proceeds of the Cybercrime received from 238 debit cards issued in several countries including USA, Canada, Brazil, Holland, Greece and some other (2) countries home and abroad. That respondents have not violated the rights of appellant in any way as to merit the grant of the reliefs (3) he sought. That appellant had not made out a case for to entitle the court to interfere with the statutory functions of the1st respondent (EFCC) to investigate the allegation of (4) crime against appellant."

See also, the unreported case of **FRN v. Okechukwu (2018)** where the court convicted Okechukwu Okoro of phishing for 2 years' imprisonment, which is a type of social engineering.

2. **Advance Fee Fraud and Other Related Offences Act, 2006:** This is another key legislation that addresses social engineering in Nigeria. The Act prohibits and punishes advance fee fraud, which often involves social engineering tactics. The Black's Law Dictionary 10th Edition states that advance fee fraud is believed to have originated in Nigeria defines the offence thus; "A criminal fraud in which the victim is persuaded by the perpetrator to pay 'fees' in anticipation of receiving a much larger benefit that is ultimately never delivered.
This law evidently prohibits and punishes advance fee fraud, which often involves social engineering tactics. For example; Section 1[15] Prohibits and punishes advance fee fraud, which often involves social engineering tactics. See, **Nwude v. F.R.N (2016) 5 NWLR (Pt. 1506) 471.**

Other relevant laws and regulations that address social engineering in Nigeria include:

1. **Economic and Financial Crimes Commission (EFCC) Act (2004**): This law establishes the EFCC and empowers[16] it to investigate and prosecute economic and financial crimes, including those involving social engineering. The decisions of the Court of Appeal in **Nwude v. F.G.N**.[17] where the EFCC prosecuted Emmanuel Nwude for advance fee fraud, which involved social engineering tactics, and the court sentenced Nwude to 25 years' imprisonment is evident that the EFCC can prosecute offenders for such crime.
Also, the Supreme Court in **Nweke v. FRN[18], Per Okoro, (J.S.C)** held;

[15] Advance Fee Fraud and Other Related Offences Act, 2004
[16] Section 46 of the EFCC Act (2004)
[17] (2004) 17 NWLR (Pt. 902) 306
[18] (2019) 10 NWLR (Pt. 1679) 51 at 69, paras. F-H; 70, paras. A-B

> **"*The Economic and Financial Crimes Commission not only has the power to investigate whether any person has committed an offence under any law relating to economic and financial crimes, it is also the co-ordinating agency for and has the power, by virtue of section 7(2) of the Act, to enforce the provisions of: the Money Laundering Act, 2004; 2003 No.7, 1995(a) No. 13; the Advance Fee Fraud and Other Related Offences(b) Act, 1995. the Failed Banks (Recovery of Debt) and Financial(c) Malpractices in Banks Act, as amended; the Banks and Other Financial Institutions Act, 1991, (d) as amended; (e) the Miscellaneous Offences Act; and any other law or regulation relating to economic and financial crimes, including the Criminal Code and(f) the Penal Code".***

2. **Nigerian Communications Commission (NCC) Act (2003).** This is the primary regulator of the telecommunications sector in Nigeria. It regulates the telecommunications sector and provides a framework for enforcing laws related to telecommunications, including those related to social engineering. In **Central Bank of Nigeria v. Ayodeji Awolola (2020)**[19]: The court convicted Ayodeji Awolola and sentenced him to 2 years' imprisonment for attempting to defraud the Central Bank of Nigeria through social engineering tactics.

3. **Criminal Code Act:** This law prohibits and punishes various crimes, including fraud, which often involves social engineering tactics. In **Imo v. State**[20] Per **(Wali J.S.C)** held;

> ***"The Criminal Code is exhaustive as to the offences and defences provided therein, and in construing its provisions recourse for assistance need not be had to English decisions or common law concepts in existence before its enactment. [Odu v. State (1965) 1 All NLR 25"***

4. **The Central Bank of Nigeria (CBN) Act, 2007**: This Act establishes the CBN as the primary regulator of the financial sector in Nigeria. The CBN has issued guidelines and regulations to combat social engineering in the financial sector.

5. **The National Information Technology Development Agency (NITDA) Act, 2007**: This Act establishes NITDA as the primary regulator of the information technology sector in Nigeria. NITDA has issued guidelines and regulations to combat social engineering in the information technology sector.

19

20 (1991) 9 NWLR (Pt. 213) 1 at 25, Para E-F.

These laws and regulations provide a framework for combating social engineering in Nigeria. However, there is a need for more effective enforcement and coordination among regulatory agencies to combat social engineering effectively.

1V. CHALLENGES IN LEGAL ENFORCEMENT OF SOCIAL ENGINEERING LAWS IN NIGERIA

Despite the efforts to combat social engineering in Nigeria, there are several challenges that hinder the effectiveness of these efforts. There are technical, legal, and institutional challenges in combating social engineering in Nigeria.

- **Technical Challenges**

a) Lack of Cybersecurity Infrastructure: Many organizations in Nigeria lack basic cybersecurity infrastructure, making them vulnerable to social engineering attacks.
b) Limited Cybersecurity Awareness: There is a lack of awareness about cybersecurity and social engineering among individuals and organizations in Nigeria.
c) Inadequate Incident Response: Many organizations in Nigeria lack incident response plans, making it difficult to respond to social engineering attacks effectively.
d) Rapidly Evolving Threat Landscape: Social engineering threats are rapidly evolving, making it challenging for organizations in Nigeria to keep up with the latest threats.

- **Legal Challenges**

a) Challenges in the Judicial System

1. Backlog of cases: Overcrowded court dockets lead to delays in hearing and resolving cases.
2. Inadequate judicial infrastructure: Insufficient court facilities, equipment, and personnel hinder efficient justice delivery.
3. Corruption: Corruption within the judiciary can compromise the integrity of the legal process.
4. Lack of specialized courts: Inadequate specialized courts for specific offenses, such as cybercrime, can lead to ineffective justice delivery.

b) Challenges in Law Enforcement

1. Inadequate training and resources: Law enforcement agencies often lack the necessary training, equipment, and resources to effectively investigate and prosecute crimes.
2. Corruption: Corruption within law enforcement agencies can compromise investigations and prosecutions.
3. Limited forensic capabilities: Inadequate forensic capabilities can hinder effective investigation and prosecution of crimes[21].
4. Jurisdictional Issues: Social engineering attacks often involve perpetrators from other countries, making it challenging for Nigerian authorities to prosecute them.

c) Challenges in Legislation

1. Outdated laws: Laws may not be up-to-date with emerging trends and technologies, making it challenging to effectively prosecute modern crimes.
2. Inadequate laws: Laws may not provide sufficient penalties or deterrents for certain crimes, leading to inadequate justice.
3. Conflicting laws: Conflicting laws and regulations can create uncertainty and hinder effective enforcement.

d) Challenges in International Cooperation

1. Limited international cooperation: Nigeria may face challenges in collaborating with international partners to investigate and prosecute transnational crimes.
2. Different legal frameworks: Nigeria's legal framework may differ significantly from those of other countries, creating challenges in international cooperation.

- **Institutional Challenges**

1. Lack of Capacity: Many organizations in Nigeria lack the capacity to combat social engineering effectively, including a lack of skilled personnel and resources.
2. Inadequate Funding: Combating social engineering requires significant funding, which is often lacking in Nigeria.
3. Limited Public Awareness: There is a lack of public awareness about social engineering in Nigeria, making it challenging to educate individuals and organizations about the risks and consequences of social engineering.
4. Corruption: Corruption is a significant challenge in Nigeria, and it can hinder efforts to combat social engineering.

Other Challenges:

[21] Data Protection in Nigeria: A Review of the Current Framework" by the Nigerian Bar Association (2020)

1. **Cultural and social factors**: Cultural and social factors, such as a lack of trust in the justice system, can hinder effective legal enforcement.
2. **Economic constraints:** Economic constraints, such as limited funding and resources, can hinder effective legal enforcement.
3. **Infrastructure challenges:** Infrastructure challenges, such as inadequate transportation and communication networks, can hinder effective legal enforcement.

Addressing these challenges requires a multi-faceted approach, including:
1. **Judicial reform:** Reforming the judicial system to improve efficiency and reduce corruption.
2. **Law enforcement reform:** Reforming law enforcement agencies to improve training, resources, and accountability.
3. **Legislative reform:** Updating laws to reflect emerging trends and technologies.
4. **International cooperation:** Strengthening international cooperation to combat transnational crimes.
5. **Public awareness and education:** Educating the public about the importance of respecting the law and the consequences of crime.

V. ACCOUNTABILITY MECHANISMS

To combat social engineering effectively in Nigeria, a multi-faceted approach is necessary. A robust accountability mechanism is crucial in ensuring that individuals and organizations are held responsible for their actions. This can be achieved through:
1. Strict Liability: Organizations should be held strictly liable for social engineering attacks that occur due to their negligence or failure to implement adequate security measures.
2. Mandatory Reporting: Organizations should be required to report social engineering incidents to the relevant authorities within a specified timeframe.
3. Sanctions and Penalties: Sanctions and penalties should be imposed on individuals and organizations found guilty of social engineering or negligence.

However, the **path to accountability Recommendations** in the context of social engineering and technology law integration in Nigeria involves several key steps:

a) Development of Specialized Courts and Tribunals

1. Establish specialized court: Establish specialized courts to handle social engineering cases, ensuring that judges and prosecutors have the necessary expertise and training.

2. Designate tribunals: Designate tribunals to handle social engineering cases, providing a faster and more efficient way to resolve disputes.
3. Provide resources: Provide resources, including funding, personnel, and infrastructure, to support the specialized courts and tribunals.

b) Alternative Dispute Resolution (ADR)

1. Explore other forms of ADR for a faster and quicker resolution of disputes if they arise.

c) Updating Laws and Regulations

1. Review and update laws: Review and update existing laws and regulations to ensure they are effective in combating social engineering.
2. Strengthen penalties: Strengthen penalties for social engineering offenses to deter perpetrators.
3. Provide clear guidelines: Provide clear guidelines and regulations for organizations to follow in preventing and responding to social engineering attacks.

d) Immediate Response

1. Incident reporting: Establish a clear process for reporting social engineering incidents to law enforcement agencies and regulatory bodies.
2. Incident response: Develop and implement incident response plans to quickly respond to social engineering attacks and minimize damage.

e) Investigation and Prosecution

1. Forensic investigation: Conduct thorough forensic investigations to gather evidence and identify perpetrators.
2. Prosecution: Prosecute social engineering cases under relevant laws, such as the Cybercrime Act and the Advance Fee Fraud Act.

f) Accountability Mechanisms

1. Regulatory oversight: Establish regulatory bodies to oversee and monitor compliance with laws and regulations related to social engineering.
2. Sanctions and penalties: Impose sanctions and penalties on individuals and organizations that engage in social engineering activities.

3. Restorative justice: Implement restorative justice mechanisms to provide remedies to victims of social engineering.

g) Preventive Measures (Promoting Public Awareness)

1. Launch Public awareness Campaigns: Conduct public awareness campaigns to educate individuals and organizations about social engineering tactics and risks.
2. Capacity building: Provide training and capacity-building programs for law enforcement agencies, regulatory bodies, and other stakeholders.
3. Technological solutions: Implement technological solutions, such as anti-phishing software and two-factor authentication, to prevent social engineering attacks.
4. Collaborate with stakeholders: Collaborate with stakeholders, including organizations, civil society groups, and community leaders, to promote public awareness.
5. Develop educational materials: Develop educational materials, including brochures, posters, and videos, to educate individuals and organizations about social engineering.

h) International Cooperation

1. International partnerships: Establish partnerships with international organizations and countries to share best practices and coordinate efforts to combat social engineering.
2. Extradition agreements: Establish extradition agreements with other countries to facilitate the prosecution of social engineering cases that involve international perpetrators.
3. Share best practices: Share best practices and lessons learned with other countries to combat social engineering.
4. Participate in international forums: Participate in international forums and conferences to discuss social engineering and cybersecurity issues.

By adhering to these paths to accountability, Nigeria can effectively combat social engineering and promote a safer and more secure online environment.

VI. CONCLUSION

Indeed! Social engineering poses a significant threat to individuals, organizations, and governments in Nigeria. Thus, A;

Balance Between Regulation and Innovation: A legal framework should encourage cybersecurity innovation while ensuring robust protection for individuals.
There needs to be Shared Responsibility: Governments, businesses, and individuals all have a role to play in preventing social engineering and ensuring accountability.
Path to a Secure Future: With a strong legal framework and increased accountability, society can move toward a future where social engineering risks are minimized.

Recommendations

1. The Nigerian government should establish a specialized cybercrime agency to investigate and prosecute social engineering cases.
2. The National Assembly should enact comprehensive legislation on social engineering, including data protection regulations and sanctions for non-compliance. Thus, Policymakers should strengthen the legal framework for combating social engineering in Nigeria, including updating laws and regulations and providing clearer guidelines for organizations.
3. Organizations should prioritize cybersecurity and implement robust measures to prevent social engineering attacks.
4. Public awareness campaigns should be launched to educate individuals on the dangers of social engineering and how to protect themselves and enhance international cooperation.

A strong and enforceable legal framework is essential in combating these threats[22]. By establishing a holistic approach with clear guidelines, regulations, and accountability mechanisms, Nigeria can create a safer digital environment and promote a culture of accountability.

[22] Social Engineering: A Growing Threat" by the Nigerian Communications Commission (2020)

SOURCES

1. Criminal Code Act (1990)
2. Cybercrime (Prohibition, Prevention, etc.) Act (2015)
3. Advance Fee Fraud and Other Related Offences Act (2006)
4. the Advance Fee Fraud and Other Fraud Related Offences Act, 2004)
5. Section 46 of the EFCC Act (2004)
6. Nigerian Communications Commission (NCC) Act (2003)
7. Lagos State High Court (Civil Procedure) Rules 2019
8. Economic and Financial Crimes Commission (EFCC) Act (2004)
9. Federal High Court (Civil Procedure) Rules 2009

BIBLIOGRAPHY

1. "Social Engineering: A Growing Threat" by the Nigerian Communications Commission (2020)
2. "Cybercrime in Nigeria: Challenges and Prospects" by the Nigerian Institute of Advanced Legal Studies (2019)
3. "Data Protection in Nigeria: A Review of the Current Framework" by the Nigerian Bar Association (2020)

REFERENCES:

1. Abawajy, J. (2014). User preference of cyber security measures to protect online transactions. International Journal of Electronic Commerce, 18(2), 159-186.
2. Adeyemo, D. (2017). Cybercrime and cybersecurity in Nigeria: An appraisal of the Cybercrime (Prohibition, Prevention, etc.) Act 2015. Journal of Cybersecurity, 3(1), 1-12.
3. CBN (2020). Cybersecurity threats and risks in the Nigerian financial sector. Central Bank of Nigeria.
4. EU (2016). General Data Protection Regulation. European Union.
5. Hadnagy, C. (2010). Social engineering: The art of human hacking. Wiley Publishing.
6. Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and Applications, 20, 44-54.
7. NCC (2015). Cybercrime (Prohibition, Prevention, etc.) Act 2015. Nigerian Communications Commission.
8. USDOJ (2020). Computer Fraud and Abuse Act. United States Department of Justice.
9. KPMG. (2019). Cyber Security Survey Report.
10. NCC. (2020). 2020 Cybersecurity Threats and Trends Report.