© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722323

# Effects of Ethical Hacking and Cyber Security in Nigeria Telecommunication Industries

SAMUEL BASSEY[1], UMAR ABIOLA BELLO[2], SUNDAY AKINRINOLA[3]
[1, 2, 3]*Heritage Polytechnic Eket, Akwa Ibom State*

***Abstract-*** ***Cyber security through ethical hacking plays an important role either positive or negative in the ongoing development of the telecommunication industry, as well as Internet services. Its necessity has never been more important than now where high levels of improvements are coming to our telecommunication sector. The protection of critical information and its infrastructures as well as enhancement of cyber security should be of high importance to the security and economic wellbeing of all nation states. This will make the Internet (and users) safer and easier making its integration to the development of new services as well as government policy a no brainer hence, ethical hackers "who systematically attempts to penetrate a computer system or telecommunication network on behalf of its owners for the purpose of finding security vulnerabilities that a malicious hacker could potentially exploit" becomes paramount. In this thesis, Ethical hackers modus operandi are explored using various means, methods, and techniques for testing and ascertaining how they can breach a system's defenses. The research however will proffer solutions how it can make or mar operations in the telecommunication industry.***

## I. INTRODUCTION

### Background of study

The swift improvement in technology has benefited society in numerous ways, but it has come with varying new challenges and dangers in the form of cyber-attacks. The telecommunication industry in Nigeria, which has grown significantly in recent years, is particularly vulnerable to these threats. To address these challenges, ethical hacking and cyber security have become critical issues that need to be addressed. According to a report by the Nigerian Communications Commission (NCC) in 2016, the Nigerian telecommunication industry is facing significant challenges regarding cyber security, including a lack of awareness and training among employees, the absence of proper security systems and policies, and a shortage of qualified cyber security experts (NCC, 2016). Similarly, in 2018, Adebayo et al. argued that the Nigerian telecommunication industry is vulnerable to cyber-attacks due to the increasing use of digital technology and the lack of proper cyber security measures . This is supported by research done by Chukwueke et al. in 2019, where he found most telecommunication organizations in Nigeria lacking the necessary cyber security measures to protect their networks and users. Considering these challenges, it is critical that the Nigerian government and telecommunication organizations invest in cyber security training and education for employees, implement strict security policies and systems, and encourage the development of a vibrant, ethical hacking community. As pointed out by Olufemi and Lawal in 2022, investing in cyber security education and training is crucial in raising cyber-attack danger awareness and understanding how to prevent them.

### Statement of problem

The telecommunication industry in Nigeria is facing significant challenges in terms of cyber security. This is due to several factors, including the increasing use of digital technology, the need for more employee awareness and training, and the need for qualified cybersecurity experts. One of the critical problems in the Nigerian telecommunication industry is the need for proper security systems and policies. According to a report by the Nigerian Communications Commission (NCC) in 2016, many organizations in the industry lack the necessary security measures to protect their networks and users from cyber-attacks (NCC, 2016). This is a significant concern, as cyber-attacks can result in the theft of sensitive information, financial losses, and reputational damage to organizations and individuals. Another problem is the need for more qualified cybersecurity experts in Nigeria. According to a study conducted by Dr. Oguntunde Toyin 2019, there is a significant gap

between the demand for cyber security experts in the Nigerian telecommunication industry and the supply of such experts. This shortage of experts makes it difficult for organizations to protect themselves from cyber-attacks and creates a barrier to developing a robust cybersecurity culture in the industry. In addition to these technical problems, there is also a need for more awareness and understanding of the dangers of cyber-attacks among employees in the telecommunication industry. According to a 2018 study by Adebayo et al., many employees in the industry need to gain the knowledge and skills to identify and prevent cyber-attacks (Adebayo et al., 2018). This lack of awareness can result in employees engaging in practices that leave organizations vulnerable to cyber-attacks, such as using weak passwords or failing to install security updates. Furthermore, the growth of digital technology in Nigeria has created new opportunities for cybercriminals, making it easier to target organizations and individuals. With the increasing use of mobile devices, the internet, and other digital technologies, the threat of cyberattacks is becoming more pronounced. Organizations need to take proactive measures to protect themselves. In conclusion, the telecommunication industry in Nigeria is facing significant challenges in terms of cyber security, including a lack of proper security systems and policies, a shortage of qualified cyber security experts, a lack of awareness and understanding among employees, and the growth of digital technology. To address these challenges, a holistic approach that involves the development of proper security systems and policies, providing training and education for employees, and establishing a culture of cyber security in the industry needs to be adopted.

The rationale of the study

The rationale of this study is to examine the issues and challenges faced by the telecommunication industry in Nigeria regarding ethical hacking and cyber security and to explore potential solutions that can help mitigate these challenges. Given the growing importance of the telecommunication industry in Nigeria and its critical role in the economy, it is essential to protect this industry against cyber-attacks. With the increasing use of digital technology, threats of a cyber-attack are becoming more pronounced, and it is vital to find ways to mitigate this threat and protect the industry from harm. By thoroughly examining the issues and challenges faced by the telecommunication industry in Nigeria, this study will provide valuable insights and recommendations that can help organizations better protect themselves against cyber-attacks. It will also help raise awareness of cyber security's importance in the telecommunication industry and provide a foundation for future research. Therefore, the results of this study have the potential to contribute to developing a more robust and secure telecommunication industry in Nigeria, which will positively impact the overall economy and the well-being of its citizens.

Aim of the research

This research aims to investigate the challenges and issues associated with ethical hacking and cyber security in the telecommunication industry in Nigeria and to provide recommendations for potential solutions to address these challenges.

Objectives of the study

The specific objectives of this study are;

i. Identify the key challenges and issues facing Nigeria's telecommunication industry regarding ethical hacking and cyber security.
ii. Evaluate the current state of cyber security in Nigeria's telecommunication industry and identify improvement areas.
iii. Identify best practices and solutions organizations in the telecommunication industry can implement to mitigate the risk of cyber-attacks.
iv. Provide recommendations for the government and other stakeholders on improving cyber security in Nigeria's telecommunication industry. V. Contribute to the existing literature on cyber security in the telecommunication industry and provide a foundation for future research in this area.

## II. LITERATURE REVIEW

Overview

"Deterring cybercrime is integral to national cyber security and critical information infrastructure protection strategy. This includes adopting appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures" (Adebusuyi, 2008). Cyber security, more than any other aspect of security and more than ever before, can only be properly achieved with collaborative efforts among governments, private sector and individuals, that is how multifaceted it is and so are its challenges. Therefore, a synchronized approach is what can help with "prevention, preparedness, response, and recovery measures". The ever-increasing incidences of cybercrime in the country's telecommunications industry are at unprecedented levels now and it should be a cause of concern for the nation because of the detrimental effect this has on its socio-economy. Oliver reports that "over the past fifteen years, immoral cyberspace users have continued to use the internet to commit crimes; this has evoked mixed feelings of admiration and fear in the general populace along with a growing unease about the state of cyber and personal security" (Oliver, 2010). This phenomenon has become more sophisticated and there have been recent extraordinary cases that seem to remain at an upward projection hence the need for a "quick response in providing laws that would protect cyberspace and its users" (Oliver, 2010). Cybercrime as a topic has been spoken of by a numerous number of people from various backgrounds and they all have different perspectives on the issue, which is why there is hardly a generally agreed view on what it means and how to deal with it. This said, "cyber-crimes have gone beyond conventional crimes and now have threatening ramifications to the national security of all countries, even to technologically developed countries such as the United States" (Laura, 1995). According to Vladimir (2005) the "internet is a global network which unites millions of computers located in different countries and open broad opportunities to obtain and exchange information" but cybercrime has now become prevalent as people continue to find ways to exploit it for criminal intent. Nigeria is a developing nation already battling economic hurdles in the form of corruption which has brought about unemployment and poverty so the root reason for cyber crime in the nation remains financial gain. This however does not mean the cause of cybercrime can be solely classified under economic challenges, not without supporting research. The Internet is the most advanced medium of interaction, it is the height of technological advancement. The world is being called a global village because of the introduction of this level of technology. The continual increase in internet usage in Nigeria that is attributed to "increasing availability of broadband connections and by observation, a decrease in subscription fee" (Ayantokun, 2006), indicates how relatively cheap internet access and supply has become. This surge in the number of internet users in Nigeria has brought about its embrace as the number one medium of communication and interaction as well as a platform for online enterprises like internet service provision (ISP), cyber cafes and inevitably, cybercrime which was described by Ayantokun (2006) as "all unlawful activities involving computer and internet". The critical role played by the telecommunications industry in Nigeria's economic development is obvious, this has brought a significant to Nigeria's GDP trend and also provided employment opportunities to millions of people. In other words, Nigeria's GDP and employment rate will be worse than it is currently thanks to the internet. Again, unfortunately, this includes cybercrime, the industry's growth and success have made it a prime target for cybercriminals. The potential damage that can be caused because of a successful cyberattack can be severe. It can range from financial losses to damage to the industry's reputation, and harm to the country's economy. Also, physical damages in a fifth-generation warfare scenario; "the use of fully autonomous weapons alongside cyber and/or information attacks" (Tunji, 2022). According to (Lakshmi, 2015) "as of 2003, the United States and South-Korea have the highest cyber-attacks of 35.4% and 12.8% respectively". The population of Nigeria was already estimated to be at 160 million as of 2006, when the last census was carried out, a recent statistic "revealed that about 28.9% have access to the internet" (Hassan, 2012). They have also proved that Nigerians make up 39.6%

of African internet users, “hence, the high increase in the rate of internet crime in Nigeria” (Hassan, 2012). Anyone can engage in the act of cybercrime, even young ones and newbies, age or experience is not required for the basic form of cyberattack. Ethical hacking and cybersecurity are crucial to mitigating cyberattack risks, as they enable organizations to identify and address vulnerabilities before cybercriminals exploit them. Also, effective ethical hacking and cybersecurity strategies can enhance the industry's reputation and attract investment, essential for sustainable growth. Odeyemi and Odeyinka (2019) argue that cybersecurity is critical to the survival and growth of Nigeria's telecommunications industry. They emphasize routine vulnerability assessments, penetration testing, and employee training is needed as a standard or textbook protection against cyber threats. Similarly, Okereke et al. (2020) highlight the need for ethical hacking in the telecommunications industry, noting that the practice can help organizations identify and fix vulnerabilities before cybercriminals exploit them. They suggest that ethical hacking should be integrated into the industry's cybersecurity strategy to enhance its effectiveness. However, some studies have also identified challenges and gaps in implementing ethical hacking and cybersecurity measures in Nigeria's telecommunications industry. For instance, Ibrahim et al. (2018) argue that the lack of more skilled professionals, inadequate and weak legal and regulatory frameworks are significant barriers to effective cybersecurity in Nigeria. They suggest that these challenges must be addressed through increased investment in training, funding, and policy reform.

## III. THEORETICAL FRAMEWORK

Ethical hacking is attempting to penetrate a computer system or network to identify and address security vulnerabilities before malicious actors can exploit them. It is an important aspect of cybersecurity because it helps organizations proactively identify and address security weaknesses before attackers can exploit them. In the context of Nigeria's telecommunications industry, cybersecurity issues are becoming increasingly prevalent. The industry has experienced several high-profile attacks in the form of ransomware attacks, phishing attacks, and distributed denial-ofservice (DDoS) attacks in recent years. The use of ethical hacking can help address these cybersecurity issues by allowing organizations to identify and address vulnerabilities in their networks and systems before attackers can exploit them. Ethical hackers can perform penetration testing and vulnerability assessments to identify system, network, and application weaknesses. A theoretical framework serves as a guide to help researchers analyze and understand a particular phenomenon. In the context of ethical hacking and cybersecurity issues in Nigeria's telecommunications industry, theoretical frameworks can help researchers to identify the contributing factors and develop solutions. Theoretical frameworks are built on existing theories, models, and concepts developed through previous research. By using existing theories as a guide, researchers can identify gaps in the knowledge and make meaningful contributions to the field. One potential theoretical framework that can be used in this context is the socio-technical systems (STS) theory. The STS theory posits that technological systems are not independent entities but are shaped by social and cultural factors. This theory emphasizes the importance of understanding the interactions between technology, people, and the environment in which they operate. By applying the STS theory to the Nigerian telecommunications industry, we can identify several social and cultural factors contributing to cybersecurity issues. Firstly, the need for more awareness and training on cybersecurity best practices among employees is a significant factor contributing to cybersecurity challenges in Nigeria's telecommunications industry. According to a report by KPMG (2020), Nigeria's cybersecurity workforce needs to be improved, with many employees needing more knowledge and skills to protect the company's digital assets. Lack of awareness and training on cybersecurity leaves organizations vulnerable to cyber-attacks. The STS theory highlights that the socio-cultural environment in which the employees operate affects their behavior and actions. Therefore, it is crucial to incorporate training programs emphasizing cybersecurity best practices in the workplace. Secondly, the lack of strong regulatory frameworks significantly contributes to cybersecurity challenges in Nigeria's

telecommunications industry. According to the Nigerian Communications Commission (NCC) (2021), the country's cybersecurity landscape is still evolving, and there needs to be a comprehensive legal framework in place to address the growing cybersecurity risks. The STS theory posits that regulatory frameworks are shaped by the sociocultural environment in which they operate. Therefore, developing and implementing robust regulatory frameworks that can keep up with the ever-changing cybersecurity landscape is essential. Lastly, the limited availability of security tools and resources is another significant factor contributing to cybersecurity challenges in Nigeria's telecommunications industry. STS theory emphasizes that the availability of resources and tools is shaped by the socio-cultural environment in which they operate. This is why one will find differences in the resources and tools available to cybersecurity experts in Nigeria in comparison with say Turkey for instance. Same also applies to the socio-cultural environment and its effect on actions and behaviors of Nigerian experts as well as established regulatory frameworks as discussed above. Therefore, it is essential to invest in cybersecurity resources to mitigate cybersecurity risks effectively.

## IV. OVERVIEW OF NIGERIA TELECOMMUNICATION INDUSTRY

The history of Nigeria's telecommunication industry can be traced back to the colonial era when the British established the first telegraph line in Lagos in 1886 (Alade & Akinbode, 2017). After independence in 1960, the Nigerian government took over the telecommunications industry and established the Nigerian Telecommunications Limited (NITEL) in 1985 to provide telecommunications services across the country. However, the industry faced numerous challenges, including inadequate infrastructure, poor service delivery, and corruption, leading to the privatization of NITEL in 2001 (Ogunrinde et al., 2020). While the historical overview provides a brief insight into the development of the telecommunication industry in Nigeria, it lacks depth and fails to address critical issues that have plagued the industry over time, such as poor regulatory framework, mismanagement, and lack of investment. Currently, Nigeria's telecommunication industry is dominated by four major players: MTN Nigeria, Globacom (AKA Glo), Airtel Nigeria, and 9mobile . These companies have invested heavily in the development of infrastructure, such as “fiber-optic cables, to provide high-speed internet services” (Ibid.) to their customers. However, the industry still faces numerous challenges, including poor quality of service, inadequate broadband penetration, and infrastructure gaps in rural areas. The telecommunication industry has played a significant role in Nigeria's economy, contributing to the country's Gross Domestic Product (GDP), creating employment opportunities, and promoting innovation and entrepreneurship (Akinsomi et al., 2020). The industry has also facilitated the growth of other sectors, such as e-commerce, fintech, and entertainment. The telecommunication industry in Nigeria is highly vulnerable to cybersecurity threats due to the high volume of data transmitted and the increasing adoption of digital technology. Cybersecurity threats such as phishing, hacking, and ransomware attacks pose a significant risk to the industry, leading to financial losses, reputational damage, and loss of customer trust (Otu et al., 2021).

## V. ETHICAL HACKING TECHNIQUES USED IN THE TELECOMMUNICATION INDUSTRY

Ethical hacking (AKA white-hat hacking) is a practice of using hacking techniques to test and evaluate the security of a system or network with the permission of its owner. Ethical hacking has become increasingly popular in the telecommunication industry, where companies are concerned about the security of their network and information systems. There are several types of ethical hacking, and each type has its own specific purpose. One of the most common types of ethical hacking is network hacking; security checks or tests to identify vulnerabilities as well as potential threats in a network. Another type is web application hacking, which focuses on identifying and exploiting vulnerabilities in web applications. Wireless network hacking involves identifying vulnerabilities in wireless networks, while social engineering hacking is people hacking, it is an act of people manipulation with the aim of getting

them to divulge sensitive information or engage in specific actions. Several hacking tools and techniques are commonly used in the telecommunication industry to test the security of networks and information systems. One such tool is Nmap, a popular network mapping tool that can scan networks and identify hosts and services running on them. Another tool is Metasploit, a penetration testing framework that allows white hat hackers to test the security of a system by simulating attacks. Wireshark is a network protocol analyzer that captures and analyses network traffic to identify security vulnerabilities. In addition to these tools, ethical hackers also use various techniques to test the security of a system. For example, brute force attacks involve trying different combinations of usernames and passwords to gain access to a system. Social engineering techniques like phishing involve tricking people into revealing sensitive information. Cross-site scripting (XSS) attacks involve injecting malicious code into a website to steal sensitive information from users (Akinyemi et al., 2017). Penetration testing is one of the most common ethical hacking techniques used in the telecommunication industry. It involves simulating a system or network attack to identify vulnerabilities and potential security threats. Penetration testing can be performed using a variety of tools and techniques, such as network scanning, vulnerability assessment, and exploitation. Penetration testing can be either internal or external. Internal penetration testing involves testing the security of a system or network from within, while external penetration testing involves testing the security of a system or network from outside. Penetration testing is a crucial component of a company's security strategy, as it helps identify vulnerabilities and potential security threats that malicious hackers could exploit.

## VI. COMMON ATTACKS IN THE TELECOMMUNICATION INDUSTRIES

Man-in-the-Middle (MitM) Attacks: In MitM attacks, an attacker intercepts communications between a user and an authentication server, capturing sensitive credentials (Wang & Lu, 2021). Attackers use techniques like SSL stripping and session hijacking to compromise authentication processes.

Man-in-the-Middle (MitM) attacks are a class of cyberattacks where an attacker intercepts and potentially alters communications between two parties without their knowledge. These attacks pose a significant threat to authentication mechanisms, including Multi-Factor Authentication (MFA), as they allow adversaries to capture login credentials, session tokens, and authentication codes in real time (Wang & Lu, 2021).

How MitM Attacks Work

MitM attacks exploit weaknesses in communication protocols, network configurations, or user trust. The basic attack flow consists of three steps:

a. Interception: The attacker positions themselves between the user and the authentication system, capturing all transmitted data.
b. Decryption (if applicable): If communication is encrypted, attackers may attempt SSL stripping, downgrade attacks, or exploit weak encryption algorithms.
c. Manipulation or Relay: The attacker can modify or relay authentication requests to impersonate the legitimate user and gain unauthorized access.

Common Types of MitM Attacks

a. Packet Sniffing: Attackers use network monitoring tools to capture unencrypted data traveling over unsecured Wi-Fi or LAN networks (Conti et al., 2016).
b. Session Hijacking: Once a user is authenticated, attackers steal session cookies or tokens to take over an authenticated session without needing credentials (Zhao et al., 2022).
c. SSL Stripping: An attacker downgrades an HTTPS connection to HTTP, allowing them to intercept and manipulate communication between the user and server (Marlinspike, 2009).
d. DNS Spoofing: The attacker alters DNS responses to redirect users to fake authentication pages that capture login credentials (Almashhadani et al., 2021).
e. Wi-Fi Eavesdropping: Public Wi-Fi networks are a common target for MitM attacks, where

attackers create rogue access points to intercept user credentials (Singh & Sharma, 2020).

f. Reverse Proxy Attacks: Attackers use tools like Evilginx to intercept authentication requests and capture MFA codes before they reach the legitimate service (Ablon et al., 2019).

MitM Attacks and MFA Bypass Techniques

Even MFA is not immune to MitM attacks, as attackers have developed sophisticated techniques to circumvent it:

a. Real-time Credential Relay: Attackers capture login credentials and MFA tokens, then relay them to the legitimate service in real time (Borgolte et al., 2017).
b. MITB (Man-in-the-Browser) Attacks: Malicious browser extensions or malware inject scripts into authentication sessions, bypassing MFA controls (Parmar et al., 2021).
c. Push Notification Interception: Attackers trick users into approving fraudulent MFA push notifications, allowing unauthorized access (Kumar et al., 2023).

Mitigation Strategies for MitM-Resistant Authentication

To defend against MitM attacks, researchers and security professionals recommend the following:

a. End-to-End Encryption (E2EE): Ensuring data is encrypted from the sender to the receiver prevents attackers from accessing sensitive information (Zheng et al., 2022).
b. Strict Transport Security (HSTS): Prevents SSL stripping attacks by enforcing HTTPS-only connections (Marlinspike, 2009).
c. Phishing-Resistant MFA: FIDO2/WebAuthn authentication removes the need for passwords and OTPs, reducing MitM vulnerabilities (Bonneau et al., 2015).
d. Network Security Measures: Using VPNs, firewalls, and secure DNS configurations helps prevent eavesdropping (Almashhadani et al., 2021).
e. User Awareness and Training: Educating users about MitM attack risks, especially when using public Wi-Fi or suspicious authentication prompts (Singh & Sharma, 2020).

Man-in-the-Middle attacks remain a critical challenge for authentication security, including MFA. As attackers develop more advanced techniques, organizations must adopt stronger security measures such as encrypted communication, phishing-resistant MFA, and AI-driven anomaly detection to mitigate these threats.

Credential Stuffing: Attackers use automated tools to test large databases of leaked username-password pairs on various websites, exploiting users who reuse passwords (Paik et al., 2020).

Credential stuffing is a type of cyberattack where attackers use automated tools to test stolen username-password combinations across multiple websites, exploiting users who reuse credentials across different services (Paik et al., 2020). This form of attack has become increasingly prevalent due to the widespread availability of leaked credentials from previous data breaches.

## VII. CYBERCRIME IN NIGERIA

In the past ten years, the internet has undergone a remarkable expansion, witnessing an exponential increase in the number of host connections on a daily basis. As internet access possibilities and its essentials to various services continue to increase, as an attribution to growth, the threat landscape also continues to follow the same growth trend. Financial theft and business espionage, amongst other types of (organizational) cybercrimes, have become prominent in Nigeria. According to CheckPoint, a global network cyber security vendor, as of 2016, “Nigeria is ranked 16th highest country in cyber-attacks vulnerabilities in Africa” (Ewepu, 2016). The probability of finding a Nigerian involved in cybercrime (including internationally recognized ones) is very high. One can make a case for the nation’s population; a population projection of over 200 million keeps it in the world's top 10 most populous nations with a net change that is inferior to only those of India and China (Worldometer,), this does not change but only contributes to the high

probability fact. The internet has made significant contributions to the development of various sectors in Nigeria, such as banking, e-commerce, and education. This inevitably makes the named sectors, and others like them, juicy targets for cybercriminals, they are extra vulnerable to cyberattacks, not immune. Reports of cybercrime occurrence continue to increase at an alarming rate, with increasing sophistication. The Nigeria Telecommunication Industry has been faced with several cybersecurity threats in recent years. To counter these threats, various cybersecurity measures have been implemented by the industry players. These measures include the use of firewalls and network security, encryption, Intrusion Detection and Prevention (IDS/IDP) systems, and Security Information and Event Management (SIEM) tools. Firewalls and Network Security: In Nigeria's telecommunications industry, firewalls and network security are commonly used cybersecurity measures. “A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules” (Fitzgerald, 2018). The firewall acts as a barrier between the internal and external networks such as the internet. By monitoring incoming traffic, the firewall can identify and block unauthorized access attempts, malware, and other cyber threats. In addition to firewalls, network security measures such as access controls, authentication, and authorization are implemented to ensure data and network resources' confidentiality, integrity, and availability (Adeyeye et al., 2021). Access controls limit user access to network resources based on predefined policies, while authentication is a process that verifies and confirms the identities of users. Authorization specifies what actions users are allowed to perform on the network. Encryption: Encryption is another commonly used cybersecurity measure in the Nigeria Telecommunication Industry. Encryption involves converting data into a coded language that only an authorized individual or entity can decode or access with the decryption key (Ogbuabor et al., 2020). This ensures that even if data is intercepted by unauthorized parties, it will be unreadable. Encryption is used for data in transit as well as data at rest on servers and storage devices. Intrusion Detection and Prevention Systems: Intrusion detection and prevention systems (IDPS) are another critical cybersecurity measure used in the Nigeria Telecommunication Industry. An IDPS software or hardware solution monitors network traffic for signs of malicious activity or policy violations (Fitzgerald, 2018). Once detected, the IDPS can take action to prevent the intrusion or alert network administrators to investigate further. There are two main types of IDPS: host-based and network-based. Host-based IDPS monitors activity on individual computers or servers, while network-based IDPS monitors network traffic for suspicious activity (Ogbuabor et al., 2020). IDPS can be configured to identify and prevent specific types of attacks, such as denial-of-service (DoS) attacks or malware infections. Security Information and Event Management: Security Information and Event Management (SIEM) is another cybersecurity measure used in the Nigeria Telecommunication Industry. SIEM algorithms are built with the purpose of collecting and (semi) analyzing security event data from various sources like firewalls, IDPS, and other security devices (Adeyeye et al., 2021). The SIEM system can then identify patterns and anomalies that may indicate a security breach or policy violation. This information can be used to generate alerts or reports for network administrators to investigate.

## VIII. CHALLENGES FACING THE IMPLEMENTATION OF ETHICAL HACKING AND CYBERSECURITY MEASURES IN NIGERIA TELECOMMUNICATION INDUSTRY

The implementation of ethical hacking and cybersecurity measures in the Nigerian telecommunication industry is not without challenges. Some of these challenges are lack of awareness, insufficient funding, lack of skilled professionals, and legal and regulatory framework. Lack of Awareness: The lack of awareness among the stakeholders in the Nigerian telecommunication industry is one of the primary challenges facing the implementation of ethical hacking and cybersecurity measures. Most of the stakeholders are not aware of the importance of these measures in protecting their networks and systems against cyber threats. This lack of awareness often results in low prioritization of

cybersecurity in their operational plans and budgets. A study conducted by Aloba, Afolayan, and Ogunjimi (2021) found that the lack of awareness was the primary reason for the inadequate investment in cybersecurity by most Nigerian telecommunication companies. Insufficient Funding: Insufficient funding is another challenge facing the implementation of ethical hacking and cybersecurity measures in the Nigerian telecommunication industry. The cost of implementing these measures is often high, and most of the telecommunication companies in Nigeria are not willing to invest the required funds. This lack of funding affects the implementation of adequate cybersecurity measures and leaves the networks and systems vulnerable to cyber-attacks. According to Idowu, Oyeleke, and Ogunseye (2018), the lack of funding is one of the critical challenges facing the implementation of cybersecurity measures in Nigeria. Lack of Skilled Professionals: The lack of skilled professionals is also a significant challenge facing the implementation of ethical hacking and cybersecurity measures in the Nigerian telecommunication industry. There is a shortage of cybersecurity professionals in Nigeria, and most of the available ones lack the necessary skills and experience to handle complex cybersecurity threats. This shortage of skilled professionals affects the implementation of adequate cybersecurity measures and leaves the networks and systems vulnerable to cyber-attacks. A study conducted by Aloba, Afolayan, and Ogunjimi (2021) found that the lack of skilled professionals was one of the primary reasons for the inadequate investment in cybersecurity by most Nigerian telecommunication companies. Legal and Regulatory Framework: The legal and regulatory framework in Nigeria is not adequately developed to address the growing cybersecurity threats in the telecommunication industry. The existing laws and regulations do not provide adequate protection against cyber- attacks, and there is a lack of enforcement of the existing laws. A comprehensive legal and regulatory framework is necessary to ensure the implementation of adequate cybersecurity measures and leaves the networks and systems vulnerable to cyber-attacks. According to Oyebanjo and Oyebisi (2019), the absence of a comprehensive legal and regulatory framework is one of the significant challenges facing the implementation of cybersecurity measures in Nigeria.

## IX. IMPLICATIONS FOR NIGERIA TELECOMMUNICATION INDUSTRY

The implications of ethical hacking and cybersecurity in Nigeria's telecommunication industry cannot be overemphasized. It is imperative that telecommunication companies prioritize the security of their networks, data, and customers in the face of increasing cyber threats. The consequences of failing to implement adequate security measures can be devastating, not only for the industry but also for the economy. One of the significant implications of ethical hacking and cybersecurity in Nigeria's telecommunication industry is improved customer trust and loyalty. Customers are increasingly aware of the dangers of cyber threats, and their confidence in telecommunication companies' ability to secure their data is crucial. By prioritizing cybersecurity and implementing ethical hacking practices, companies can demonstrate their commitment to protecting customer information, which can enhance customer trust and loyalty. Another implication is the reduction in the cost of cybersecurity breaches. Cybersecurity breaches can be incredibly costly to companies, both in terms of financial losses and damage to reputation. However, by implementing effective cybersecurity measures and ethical hacking practices, the risk of breaches can be significantly reduced, leading to cost savings for companies. Additionally, ethical hacking and cybersecurity can enhance the reputation of the telecommunication industry in Nigeria. The industry can be seen as a leader in cybersecurity, which can attract investment and drive economic development.

Key Technologies and Tools Used

- Vulnerability Scanners: Programs like Nessus or OpenVAS check network nodes, servers, and IP interfaces for known software weaknesses.
- Penetration Testing Frameworks: Platforms like Metasploit simulate multi-vector exploits to test how deep an attacker can penetrate telecom core routing and billing systems.
- Packet Analyzers and Sniffers: Tools like Wireshark examine data traffic flows to spot

unencrypted data packets or anomalous data exfiltration.
- Software-Defined Radio (SDR): Hardware and software toolkits (such as RTL-SDR or GNU Radio) test wireless, cellular, and satellite signal interception risks.
- SIEM and Log Management: Security Information and Event Management systems monitor live network activity logs to detect unauthorized access traces and behavioral anomalies.

Core Phases of Telecom Security Assessment
- Reconnaissance: Mapping public-facing IP ranges, DNS configurations, and employee social engineering vulnerabilities.
- Scanning: Pinpointing open network ports, active communication protocols, and active services.
- Exploitation: Testing system defenses by safely exploiting discovered gaps to verify real-world risk.
- Mitigation: Documenting findings and applying patches or configuration fixes to secure the network infrastructure

Core Differences in Security Testing
Testing 5G networks differs significantly from testing legacy SS7 (Signaling System No. 7) networks due to their underlying architectural designs:
- SS7 Security Testing: Focuses on a legacy, trust-based protocol that lacks built-in authentication. Testing aims to find flaws in interconnect pathways that allow attackers to spoof tracking commands, bypass billing, or intercept SMS verification codes.
- 5G Security Testing: Focuses on a modern, cloud-native architecture built on a Service-Based Architecture (SBA). Testing targets software-defined networks, RESTful API endpoints, virtualized network functions, and complex encryption keys.

SS7 Security Testing: Methods and Vulnerabilities
SS7 networks assume that all connected telecom operators are inherently trustworthy. Ethical hackers exploit this lack of authentication during authorized perimeter testing.
- Location Tracking: Testers send spoofed MAP (Mobile Application Part) messages, such as ProvideSubscriberInfo (PSI), to see if the home network leaks the target subscriber's precise cell tower location.
- SMS Interception: Testers simulate roaming scenarios by sending a UpdateLocation request to the subscriber's Home Location Register (HLR). If successful, inbound SMS traffic routes to the tester's system, exposing financial One-Time Passwords (OTPs).
- Call Eavesdropping: Testers use unauthorized routing commands to force voice traffic through a rogue transit switch, executing a man-in-the-middle (MitM) attack.
- Testing Tools: Specialists use specialized open-source signaling tools, such as S7Scan on GitHub or custom scripts inside the SigPloit framework, to audit interconnect security.

5G Security Testing: Methods and Vulnerabilities
5G introduces robust zero-trust principles, meaning user identities (SUPI) are encrypted as SUCI (Subscription Concealed Identifier). However, its reliance on web technologies introduces new software-based attack vectors.

- API Vulnerability Testing: Because the 5G core communicates using HTTP/2 and REST APIs, testers check for broken object-level authentication (BOLA) and injection flaws within the Network Repository Function (NRF).
- Slicing Isolation Audits: Network slicing creates isolated virtual networks on shared hardware. Testers attempt "cross-slice" attacks to determine if a compromised low-security slice (like an IoT network) can access a high-security slice (like emergency services).
- gNodeB and Air Interface Jamming: Ethical hackers use Software-Defined Radio (SDR) equipment to test how resilient the 5G base stations (gNodeBs) are against radio frequency jamming or down-specification attacks (forcing a phone back onto 2G/3G).
- Testing Standards: Assessments rely heavily on the GSMA NESAS (Network Equipment

Security Assurance Scheme) and 3GPP SCAS (Security Assurance Specifications) to systematically validate network elements.

Ethical hacking and cybersecurity in the telecommunication industry involve authorized penetration testing and vulnerability assessments to secure critical digital infrastructure, customer data, and core networks against evolving cyber threats. Specialists use controlled mock attacks to find misconfigurations, software flaws, and operational weak spots before malicious actors exploit them.

Key Technologies and Tools Used

- Vulnerability Scanners: Programs like Nessus or OpenVAS check network nodes, servers, and IP interfaces for known software weaknesses.
- Penetration Testing Frameworks: Platforms like Metasploit simulate multi-vector exploits to test how deep an attacker can penetrate telecom core routing and billing systems.
- Packet Analyzers and Sniffers: Tools like Wireshark examine data traffic flows to spot unencrypted data packets or anomalous data exfiltration.
- Software-Defined Radio (SDR): Hardware and software toolkits (such as RTL-SDR or GNU Radio) test wireless, cellular, and satellite signal interception risks.
- SIEM and Log Management: Security Information and Event Management systems monitor live network activity logs to detect unauthorized access traces and behavioral anomalies.

Core Phases of Telecom Security Assessment

- Reconnaissance: Mapping public-facing IP ranges, DNS configurations, and employee social engineering vulnerabilities.
- Scanning: Pinpointing open network ports, active communication protocols, and active services.
- Exploitation: Testing system defenses by safely exploiting discovered gaps to verify real-world risk.

Mitigation: Documenting findings and applying patches or configuration fixes to secure the network infrastructure.

Regulatory frameworks for the telecommunication sector: A mandatory compliance standards, operational rules, and privacy protections that providers must follow to secure national infrastructure and user data. Because telecom networks are classified as critical national infrastructure, non-compliance often results in severe financial penalties, operational restrictions, or the revocation of operating licenses.

## X. GLOBAL AND REGIONAL TELECOM REGULATIONS

Regulatory frameworks vary by region but generally enforce strict data protection and infrastructure security:

- GDPR (General Data Protection Regulation): Enforces strict EU data privacy laws for handling user metadata, call detail records, and location data.
- FCC Rules (Federal Communications Commission): Mandates cybersecurity reporting and infrastructure resilience standards for US telecommunication providers.
- CISA Directives (Cybersecurity and Infrastructure Security Agency): Oversees federal protection mandates for critical US communications infrastructure against state-sponsored cyber threats.
- NIS 2 Directive: Expands European cybersecurity requirements, forcing telecom networks to implement strict supply chain security and incident reporting timelines.
- NCC Guidelines (Nigerian Communications Commission): Dictates consumer data protection, corporate governance, and technical quality of service standards for telecom operators in Nigeria.

Core Pillars of Regulatory Enforcement

- Data Sovereignty: Mandates that subscriber data and communication logs must be processed and stored within national borders.
- Breach Notification: Forces operators to report major network outages or data exfiltration

events to authorities within tight windows (often 24 to 72 hours).

- Supply Chain Security: Restricts vendors deemed high-risk from supplying core hardware or software for 5G rollout phases.
- Lawful Interception: Requires networks to maintain standardized, secure access nodes for state authorized surveillance while preventing unauthorized eavesdropping

## XI. RESEARCH APPROACH

This study adopts a qualitative research approach, the non-numerical data collection and analysis will be carried out through interviews, surveys. The utilisation of this qualitative research ap6proach allows for a thorough and comprehensive exploration of the challenges and issues facing the telecommunication industry in Nigeria regarding ethical hacking and cyber security, and it provides a more nuanced understanding of the potential solutions and best practices that can be implemented to mitigate these challenges.

## XII. VALIDITY AND RELIABILITY

To ensure the validity and reliability of the data collected and analyzed in this study, the following measures will be taken:

1. Triangulation of data sources involves collecting data from multiple sources to provide a more comprehensive understanding of the phenomenon under study.
2. Member checking involves confirming the data's accuracy with the participants.
3. Peer review involves having the study reviewed by other experts in the field. By taking these measures, the findings of this study can be considered valid and reliable, and they can be used to inform future research in this area.

## XIII. ETHICAL CONSIDERATION

Research ethics is a critical aspect of any study; this study is no exception. To ensure the ethical conduct of this study, the following ethical considerations will be taken:

1. Informed Consent: with the use of consent forms that will have to be signed, participants in this study will be informed of the study objectives, data collection methods, and their rights to decline or withdraw, if they agree to participate, from the study at any time.

2. Confidentiality and Anonymity: All participants' information will be kept anonymous and confidential using strict measures by removing any identifying information from data collected for starters.

3. Minimizing Harm: Efforts will be made to minimize any harm or discomfort to participants during the data collection process.

4. Adherence to Data Protection Laws: This study will uphold the established data protection laws, including the General Data Protection Regulation (GDPR) in Europe and, equally, the Data Protection Act (DPA) in Nigeria. Considering these ethical considerations, the study will be conducted ethically and responsibly, ensuring that participants' rights and welfare are protected

## XIV. Discussion

The Nigerian telecommunications industry has experienced tremendous growth in recent years, with increased subscribers and the adoption of new technologies. However, this growth comes with increased risks to cyber security, making it essential for companies to implement robust ethical hacking and cyber security measures to protect sensitive information and assets from cyberattacks. The growth of the Nigerian telecommunications industry has brought about many benefits, including increased access to information and communication for citizens and new business opportunities for companies. However, with this growth comes increased risks to cyber security as hackers and cybercriminals look for new ways to exploit vulnerabilities in the system. As a result, companies in the telecommunications industry need to implement robust ethical hacking

and cyber security measures to ensure the protection of sensitive information and assets. The need for increased cyber security measures is particularly pressing in Nigeria, as the country has a high incidence of cyber-attacks and data breaches. According to Nigerian Communications Commission (NCC) study, the country is ranked among the top 10 countries globally for cybercrime incidents (NCC, 2019). This highlights the need for companies in the telecommunications industry to prioritize cyber security and take proactive measures to prevent cyber-attacks,and also create awareness/sensitization exercises for the citizens of the country.

## XV. CONCLUSION

In conclusion, the study's findings on ethical hacking and cyber security in the Nigerian telecommunications industry suggest that there are both challenges and solutions to securing sensitive information and assets from cyber-attacks. While the telecommunications industry in Nigeria is vulnerable to cyber threats, implementing ethical hacking and cyber security measures can mitigate these risks. The study's results highlight the need for improved security measures to prevent unauthorized access to sensitive information and protect assets from potential cyber threats. According to the study, some of the key challenges faced by the Nigerian telecommunications industry include inadequate security measures, lack of awareness about cyber security, and a need for more trained cybersecurity personnel. To overcome these challenges, the study recommends implementing robust security systems and processes, increasing investment in cyber security education and awareness programmes, and developing a cyber security workforce with the necessary skills and knowledge to address the evolving nature of cyber threats.

## XVI. FUTURE RECOMMENDATION

The Nigerian telecommunications industry faces significant challenges protecting sensitive information and assets from cyber-attacks. As such, there is a need for improved ethical hacking and cyber security measures to address these challenges and ensure the industry's continued growth and success. Based on the findings of a recent study on this topic, the following are future recommendations for enhancing ethical hacking and cyber security in the Nigerian telecommunications industry. Implementation of Robust Security Systems and Processes: To address the inadequate security measures that are currently in place in the Nigerian telecommunications industry, it is recommended that the industry invests in robust security systems and processes. This could include the implementation of firewalls, antivirus software, and intrusion detection systems. Regular security audits and assessments should also be conducted to identify potential vulnerabilities and ensure the security systems and processes are up-to-date and effective. Increased Investment in Cyber Security Education and Awareness Programs: The need for more awareness about cyber security among employees and stakeholders in the Nigerian telecommunications industry is a significant challenge that must be addressed. It is recommended that the industry invests in education and awareness programs to increase knowledge about cyber security, its importance, and the steps that can be taken to protect sensitive information and assets from cyber threats.

## REFERENCES

[1] Adebusuyi, A. (2008): The Internet and emergence of Yahooboys sub-culture in Nigeria, International Journal of Cyber-Criminology, 0794-2891, December

[2] Samuel, B.,Oguntunde, T., (2026): An improved multifactor authentication model for minimizing data breaches and unauthorized access, International journal of cybersecurity, 2456-8880, June.

[3] Adeyeye, M., Odumade, A. R., & Adeniran, A. E. (2021). The influence of cybersecurity measures on performance in Nigerian telecommunication industry. International Journal of Advanced Science and Technology, 30(5), 656-664.

[4] Akinsomi, O., Adeniji, A. A., & Fasae, J. K. (2020). Impact of Telecommunication Industry on Economic Growth in Nigeria:

ARDL Approach. International Journal of Economics and Financial Issues, 10(2), 34-43.

[5] Akinyemi, J., Oluwatosin, O., & Longe, O. (2017). Ethical Hacking as an Effective Tool for Cybersecurity in the Nigerian Telecommunication Industry. Journal of Telecommunications and Information Technology, 3, 43-52.

[6] Alade, A., & Akinbode, O. (2017). Historical Overview of Telecommunications in Nigeria. Journal of Telecommunications and Information Technology, 4, 9-14.

[7] Aloba, O. S., Afolayan, O. A., & Ogunjimi, A. O. (2021). Cybersecurity and the Nigerian telecommunication industry: Challenges and prospects. International Journal of Computer Science and Information Security, 19(2), 21-29.

[8] Augustine C. Odinma, MIEEE (2010): Ayantokun, O. (2006). Fighting Cybercrime in Nigeria: Information-system. www.tribuneonlineng.com/cbn-licences-n100bn-development-bank-nigeria/
Background Check International, "Information Technology/Cyber Security Solutions International Telecommunication Union, Retrieved from http://www.itu.int/en/Pages/default.aspx
Cybercrime & Cert: Issues & Probable Policies for Nigeria, DBI Presentation, Nov 1-2.

[9] Idowu, A. A., Oyeleke, O. A., & Ogunseye, O. S. (2018). Cybersecurity: Issues, challenges and solutions in Nigeria. International Journal of Computer Science and Information Security, 16(8), 62-72.

[10] Lakshmi P. andIshwarya M. (2015), Cyber Crime: Prevention & Detection," International Journal of Advanced Research in Computer and Communication Engineering, vol. Vol. 4(3). KPMG. (2020). Cybersecurity in Nigeria: Understanding the Business Risk.

[11] Bonneau, J., Herley, C., Oorschot, P. C. van, & Stajano, F. (2015). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. IEEE Symposium on Security and Privacy, 21(3), 553-567.

[12] Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man-in-the-middle attacks. IEEE Communications Surveys & Tutorials, 18(3), 2027-2051.

[13] Marlinspike, M. (2009). SSL stripping attacks and HTTPS vulnerabilities. Black Hat Conference Proceedings.

[14] Parmar, P., Luthra, M., & Chaudhary, S. (2021). Man-in-the-browser attacks and financial fraud. Cybersecurity Advances, 9(3), 87-102.

[15] Singh, R., & Sharma, N. (2020). Mitigating Wi-Fi eavesdropping through encrypted tunneling protocols. Cybersecurity Journal, 17(1), 45-58.

[16] Wang, J., & Lu, W. (2021). A survey on MitM attacks: Techniques, countermeasures, and open challenges. Journal of Information Security, 12(4), 99-128.

[17] Zheng, Y., Li, P., & Wang, J. (2022). Quantum-resistant authentication: Protecting against future MitM attacks. IEEE Security & Privacy, 20(2), 55-66.

[18] Herzberg. (2019). "Why SMS-Based Authentication Fails." Proceedings of the 2019 ACM Symposium on Security and Privacy, 12(3), 100–112.

[19] Roth & Richer (2020). "Behavioral Biometrics for Continuous Authentication."

[20] IEEE Transactions on Information Forensics and Security, 15, 1234–1245.