[FRONT COVER]

CHARLES UNIVERSITY

FACULTY OF SOCIAL SCIENCES

Institute of Political Studies

Master thesis

2023 **Adetunji Akinyemi**

[title page]

CHARLES UNIVERSITY

FACULTY OF SOCIAL SCIENCES

Institute of Political Studies

Adetunji Akinyemi

ETHICAL HACKING AND CYBER SECURITY IN NIGERIA TELECOMMUNICATION INDUSTRY: ISSUES AND SOLUTION

Master thesis

Prague 2023

Author: MSc. Adetunji Akinyemi
Supervisor: doc. PhDr. Vít Střítecký, M.Phil., Ph.D.

Academic Year: 2022/2023

Bibliographic note

AKINYEMI, Adetunji. *ETHICAL HACKING AND CYBER SECURITY IN NIGERIA TELECOMMUNICATION INDUSTRY: ISSUES AND SOLUTION*. 71 p. Mater thesis. Charles University, Faculty of Social Sciences, Institute of Political Studies Supervisor doc. PhDr. Vít Střítecký, M.Phil., Ph.D.

Declaration of Authorship

1. The author hereby declares that he compiled this thesis independently, using only the listed resources and literature.

2. The author hereby declares that all the sources and literature used have been properly cited.

3. The author hereby declares that the thesis has not been used to obtain a different or the same degree.

Prague 15/7/2023 **Adetunji Akinyemi**

Acknowledgments

I would like to express my sincere gratitude to EVERY contributor, for guidance, support, and encouragement throughout the research process. I am grateful for the valuable time, constructive feedback, and invaluable advice, which has helped me shape this thesis into a better piece of work.

I am grateful to my friends back home in Nigeria, for providing me with the necessary resources and support to complete this research. I am thankful for the facilities and support services that were provided to me during the course of my research. Lastly, I would like to thank all the participants who were involved in my research. Without their time, effort, and willingness to share their experiences, this thesis would not have been possible.

I express my gratitude to all who have helped and supported me in this journey. This thesis is a testament to the support, guidance, and love I have received from them.

Proposal

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 well-being of all nation states. This will make the Internet (and users protection) 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" (Eduproject) 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.

DEDICATION

I dedicate this thesis to my loving parents, who have always been my source of inspiration and support. Their unwavering belief in me has been my driving force throughout my academic journey. I am grateful for their love, encouragement, and sacrifices they made to give me a better life. This thesis is a small token of appreciation for their sacrifices and love.

To the colleagues and eventual friends I made in Prague too, I cannot have been so inspired to finish this work without them. The little conversations, arguments and shared insights emboldened me to write on this research and finish

TABLE OF CONTENT

LIST OF TABLES

Table 11. Do you believe that Nigerian telecommunication companies are taking enough responsibility for ensuring the security of their customer's data?

Table 12. Do you believe Nigerian telecommunications companies are taking adequate steps to protect their systems from unethical hacking?

Table 14. Do you think the Nigerian government should provide more resources to improve the cyber security of its telecommunication industry?

Table 15. Do you believe international organizations should be involved in improving the cyber security of the Nigerian telecommunication industry?

Table 16. Do you think ethical hackers should be regulated in the Nigerian telecommunication industry?

Table 17. Do you believe the Nigerian telecommunication industry is taking enough steps to prevent data breaches?

Table 18. The Nigerian telecommunication industry needs to prioritize the implementation of cyber security measures.

Table 19. Ethical hacking practices effectively ensure the security of Nigeria's telecommunication industry.

Table 20. Companies in the Nigerian telecommunication industry should invest more in the training and development of their cyber security personnel.

CHAPTER ONE

INTRODUCTION

1.1 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 (Adebayo et al., 2018). 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 (Chukwueke et al., 2019).

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 and how to prevent them (Olufemi & Lawal, 2022).

1.2 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 Chukwueke et al. in 2019, there is a significant gap between the demand for cyber security experts in the Nigerian telecommunication industry and the supply of such experts (Chukwueke et al., 2019). 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 cyber-attacks 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.

1.3 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.

1.4 Research Question

The research questions for this study are;

I. What are the main issues and challenges faced by the telecommunication industry in Nigeria regarding ethical hacking and cyber security?

II. What solutions and best practices can be implemented by organizations in the telecommunication industry to mitigate the risk of cyber-attacks?

III. What role can the government play in improving the telecommunication industry in Nigeria, and what initiatives can be taken to raise awareness of cyber security?

1.5 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.

1.6 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.

CHAPTER TWO

LITERATURE REVIEW

2.1 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.

2.1.1 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-of-service (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.

2.2 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 (FKA Etisalat). 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).

2.3 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.

2.4 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 essentiality 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.

2.5 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.

2.6 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 growth.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Research Approach

According to (Bouchrika, 2022), “research methodology can be approached qualitatively or quantitatively”. However, this descriptive study will be approached quantitatively. “Quantitative research is concerned with gathering numerical data to explain a phenomenon often generalised across a group of people” (Babbie, 2010). 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 approach 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.

3.2 Research Design

This study employs a case study research design, a comprehensive examination of a particular phenomenon within its real-life context. The case study research design is utilized for this study for a detailed analysis of the telecommunication industry in Nigeria and the challenges it faces regarding ethical hacking and cyber security.

3.3 Data Collection Methods

“Data collection is gathering necessary and relevant information about a subject matter” (Cote, 2021). “Data collection enables a researcher to collect and measure data systematically through primary and secondary sources, answer the research question, test the hypothesis and evaluate findings. However, for this study, data was collected through a primary source because it provides first-hand experience in this field of research” (Kabir, 2016). In addition, the self-administered close-ended questionnaire is used in collecting data in this study. To gather statistical data and for examination, a questionnaire is used in this study. This approach enhances convenience, reduces bias, and improves data accessibility and collection. The Likert scale questionnaire format was used, presenting questions in a range of responses based on degree of acceptance; strongly agree to strongly disagree. Participants were asked to indicate their level of agreement with each statement. The questionnaire was divided into two sections: Part A collected demographic data and assessed eligibility based on predetermined eligibility criteria set, while Part B consisted of operational questions categorized according to biases in the Messy Middle model. This design facilitates the exploration of the impact of online fashion consumers' preferences.

3.4 Data Analysis Methods

After administering the questionnaire, the data gathered from respondents was put through a cleaning process with the use of MS Excel to address anomalies like inaccurate or duplicate responses. This is a descriptive type of research so descriptive statistics; employed for data presentation in frequencies and percentages for the identification of significant biases, and inferential statistics; simple linear regression, was employed for hypothesis testing to estimate, as

accurately as possible, the relationship strength between two continuous variables, were used for data analysis.

The simple Linear regression model can be represented as follows:

$y = a + bx$

Where:

a = intercept

b = slope

x = independent variable

and y = dependent variable

This chosen method of data analysis for this study is employed to aid informed decision making upon completion of the study. Version 23 of the Statistical Package for the Social Sciences (SPSS) was employed in the conducting of analysis, it can perform intricate analyses, including the descriptive and inferential statistics analysis, as well as create plots for trends.

3.5 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.

3.6 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.

CHAPTER FOUR

DATA ANALYSIS AND INTERPRETATION OF RESULT

Preamble

This chapter is for the presentation and discussion of the results of data analyzed and what this implies in the context of the study; Ethical hacking and cybersecurity in Nigeria's telecommunication industry. The aim remains to address associated issues to be identified as well as proffer solutions to these issues to be determined. 100 questionnaires were distributed, 62 questionnaires were returned and used for data analysis. Frequency distribution and percentages were the descriptive statistical tool used for the examination of the research instrument, while simple linear regression, a type of inferential statistics method of data analysis, were conducted using SPSS version 23.

4.1 The Respondent's Descriptive Characteristics

Table 1: Gender Distribution of the sample Population (N=62)

Gender	Frequency	Percentage (%)
Male	41	66.1
Female	21	33.9
Total	62	100

This table represents the gender distribution of the study population, which comprises 62 individuals. Of the 62 individuals, 41 (66.1%) are male, and 21 (33.9%) are female.

Table 2: Descriptive Statistics for Age Group (N=62)

Age Group (Years)	Frequency	Percentage (%)
18-24	22	35.5
25-30	19	30.6
31-35	14	22.6
36-40	7	11.3

The table represents the age distribution of a sample of 62 individuals. The age groups are divided into four categories: 18-24, 25-30, 31-35, and 36-40. The frequency column represents the number of individuals in each age group while the percentage column represents the proportion of individuals in each age group compared to the total sample size (N=62). The largest age group is

the 18-24 category, with 22 individuals or 35.5% of the sample. The second largest is the 25-30 age group, with 19 individuals or 30.6%.

Data Presentation and Analysis

Table 3. Do you believe Nigerian telecommunications companies are taking adequate steps to protect their systems from ethical hacking?

		Frequency	Per cent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	11	17.74	17.74	17.74
	Disagree	9	14.52	14.52	32.26
	Undecided	13	20.97	20.97	53.23
	Agree	19	30.65	30.65	83.88
	Strongly agree	10	16.13	16.13	100
	Total	62	100	100	

Of 62 respondents, 17.74% strongly disagreed that Nigerian telecommunications companies are taking adequate steps to protect their systems from ethical hacking. 14.52% disagreed, 20.97% were undecided, 30.65% agreed, and 16.13% strongly agreed. The results show that many respondents believe that Nigerian telecommunications companies need to take adequate steps to protect their systems from unauthorized access. This implies that there may be a need for more trust and confidence in the security measures put in place by these companies, which could negatively impact their reputation and customer loyalty. It also highlights the need for these companies to focus on improving their security measures to better protect against unethical hacking and earn the trust of their customers.

Table 4. Do you believe cyber security measures in the Nigerian telecommunication industry adequately prevent cyber-attacks?

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly disagree	20	32.26	32.26	32.26
Disagree	13	20.97	20.97	53.23
Undecided	8	12.90	12.90	66.13
Agree	12	19.34	19.34	85.47

	Strongly agree	9	14.52	14.52	100
Valid	Total	62	100	100	

Table 5. Has the Nigerian government done enough to improve the cyber security of its telecommunication industry?

	n	Frequency	Percent	Valid Percent	Cumulative Percent
	Strongly disagree	9	14.5%	14.5%	14.5%
	Disagree	22	35.5%	35.5%	50%
	Undecided	5	8.1%	8.1%	58.1%
	Agree	17	27.4%	27.4%	85.5%
	Strongly agree	9	14.5%	14.5%	100%
Valid	Total	62	100%	100%	100%

Out of 62 respondents, 50% disagree or strongly disagree that the Nigerian government has done enough to improve the cyber security of its telecommunication industry; 35.5% of the respondents disagree with the statement, while 14.5% strongly disagree. On the other hand, 27.4% of the respondents agree that the government has done enough, while 14.5% strongly agree. 8.1% of the respondents are undecided on the issue. The results suggest that most of the respondents are not satisfied with the efforts of the Nigerian government in the cyber security of its telecommunication industry. This highlights the need for the government to proactively address this issue and protect sensitive information in the telecommunication sector.

Table 6. Do you think the Nigerian telecommunication industry is well-equipped to respond to ethical hacking incidents and cyber-attacks?

n	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly disagree	8	12.90	12.90	12.90
Disagree	17	27.41	27.41	40.31
Undecided	4	6.45	6.45	46.76
Agree	23	37.10	37.10	83.86

Valid	Strongly agree	10	16.13	16.13	100
	Total	62	100	100	

Based on the results, most respondents (53%) either agreed or strongly agreed that the Nigerian telecommunication industry is well-equipped to respond to unethical hacking incidents and cyber-attacks. Meanwhile, 40% of the respondents disagreed or strongly disagreed with this statement. This implies that although there is stronger support and trust in the capabilities of the Nigerian telecommunications industry, there needs to be more in the respondents' perception of the capability of the Nigerian telecommunication industry in responding to cyber threats. 53% of security and customer information protection support is shaky, but it implies that the industry is doing some things right. The result suggests a need to improve the Nigerian telecommunication industry's capability to address unethical hacking incidents and cyber-attacks. This will help increase the stakeholders' confidence in the industry and promote its growth. The industry should invest more in developing its cyber-security infrastructure and hire knowledgeable personnel dealing with these threats.

Table 7. Do you think ethical hacking should be allowed in the Nigerian telecommunication industry to identify vulnerabilities in the system?

	n	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	5	8.06	8.06	8.06
	Disagree	8	12.90	12.90	20.96
	Undecided	9	14.52	14.52	35.48
	Agree	23	37.10	37.10	72.58
	Strongly Agree	17	27.42	27.42	100
	Total	62	100.00	100.00	100.00

Based on the data above, a significant number of people (65%) agree that ethical hacking should be allowed in the Nigerian telecommunication industry to identify vulnerabilities in the system. On the other hand, only a minority (20.96%) disagree with this notion. This result implies a consensus among the population on the importance of ethical hacking in ensuring the security of the telecommunication industry in Nigeria. Thus, it is highly recommended that the industry embraces ethical hacking and put measures in place to regulate it to ensure it is carried out ethically and securely.

Table 8. Do you believe that the current regulations in Nigeria regarding cyber security in the telecommunication industry are sufficient?

	n	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	20	32.2	32.2	32.2
	Disagree	14	22.6	22.6	54.8
	Undecided	10	16.1	16.1	70.9
	Agree	11	17.7	17.7	88.6
	Strongly agree	7	11.3	11.3	100
	Total	62	100	100	

Out of 62 participants, 32.2% strongly disagree with the sufficiency of the current regulations in Nigeria regarding cyber security in the telecommunication industry. A total of 54.8% either disagree or strongly disagree, indicating that most participants do not believe the current regulations are sufficient. On the other hand, 17.7% of participants agree with the sufficiency of

the regulations, while 11.3% strongly agree. This suggests a need for further review and improvement of the current regulations to ensure better protection against cyber threats in the telecommunication industry.

Table 9. Do you think the Nigerian telecommunication industry is investing enough in cyber security?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	4	6.45	6.45	6.45
	Disagree	8	12.90	12.90	19.35
	Undecided	20	32.26	32.26	51.61
	Agree	17	27.42	27.42	79.03
	Strongly agree	13	21.03	21.03	100
	Total	62	100	100	

Of the 62 respondents, 6.45% strongly disagreed that the Nigerian telecommunication industry is investing enough in cyber security. 12.90% disagreed, 32.26% were undecided, 27.42% agreed, and 21.03% strongly agreed. The results indicate that a significant portion of the respondents (51.61%) need clarification/to disagree that the telecommunication industry is investing enough in cyber security. This highlights the need for increased awareness and education on the importance of cybersecurity investment in the industry. Additionally, only a small portion of the respondents (48.39%) believed that the industry is making enough investment in cyber security, indicating that there may be a need for increased investment in this area.

Table 10. Should the public be made more aware of the risks associated with cyber security in the Nigerian telecommunication industry?

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly disagree	0	0	0	0
Disagree	2	3	3	3
Undecided	0	0	0	3
Agree	28	45.2	45.2	48.2

Valid	Strongly agree	32	51.6	51.6	100
	Total	62	100	100	

Out of the 62 respondents, 52% strongly agreed that the public should be made more aware of the risks associated with cyber security in the Nigerian telecommunication industry. 45% agreed, 3% disagreed, and 0% strongly disagreed or were undecided. The results suggest that most respondents believe raising public awareness of cyber security risks in the Nigerian telecommunication industry is important. This highlights the need for increased efforts to educate and inform the public on these issues to protect against potential cyber-attacks and threats.

Table 11. Do you believe that Nigerian telecommunication companies are taking enough responsibility for ensuring the security of their customer's data?

		Frequency	Percent	Valid Percent	Cumulative Percent
	Strongly disagree	20	32.3	32.3	32.3
	Disagree	17	27.4	27.4	59.7

Valid	Undecided	13	21.0	21.0	80.7
	Agree	4	6.5	6.5	87.1
	Strongly agree	8	12.9	12.9	100
	Total	62	100	100	

Based on the survey results, 59.7% of the respondents either strongly disagree or disagree that Nigerian telecommunication companies are responsible enough to ensure their customers' data security. This shows a high level of skepticism among the respondents towards the security measures put in place by telecommunication companies. On the other hand, 12.9% of the respondents strongly agree that the companies are taking enough responsibility. This survey highlights the need for Nigerian telecommunication companies to prioritize their customers' data security. Companies need to invest in more robust and secure data protection measures to gain the trust and confidence of their customers. Furthermore, telecommunication companies must educate their customers on the security measures they have in place and the steps they take to keep their data safe.

Table 12. Do you believe Nigerian telecommunications companies are taking adequate steps to protect their systems from unethical hacking?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	2	3.23	3.23	3.23
	Disagree	9	14.52	14.52	17.75
	Undecided	17	27.42	27.42	45.16
	Agree	23	37.10	37.10	82.26
	Strongly agree	11	17.74	17.74	100
	Total	62	100	100	

According to the data, out of 62 respondents, only 2 (3.23%) strongly disagree that Nigerian telecommunications companies are taking adequate steps to protect their systems from unethical hacking. 9 (14.52%) disagree, 17 (27.42%) are undecided, 23 (37.10%) agree, and 11 (17.74%) strongly agree. This data implies that most respondents either agree or strongly agree that Nigerian

telecommunications companies are taking adequate steps to protect their systems from ethical hacking. This shows that most of the respondents have trust and confidence in the measures put in place by these companies to protect their systems from potential threats.

Table 14. Do you think the Nigerian government should provide more resources to improve the cyber security of its telecommunication industry?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	6	9.68	9.68	9.68
	Disagree	7	11.29	11.29	20.97
	Undecided	5	8.06	8.06	29.03
	Agree	20	32.26	32.26	61.29
	Strongly agree	24	38.71	38.71	100
	Total	62	100	100	

Based on the tabular form, out of the 62 respondents, 38.71% strongly agree that the Nigerian government should provide more resources to improve the cyber security of its telecommunication industry. This implies that most respondents support the government's proactive measures to secure the telecommunication industry. On the other hand, 9.68% of the respondents strongly disagree, meaning they do not believe the government should provide more resources to improve cyber security. The remaining respondents either disagree or are undecided. Overall, the results suggest that there is a need for the government to invest in improving the cyber security of the telecommunication industry.

Table 15. Do you believe international organizations should be involved in improving the cyber security of the Nigerian telecommunication industry?

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly disagree	0	0	0	0
Disagree	2	3.23	3.23	3.23
Undecided	0	0	0	0
Agree	29	46.77	46.77	50.00

Valid	Strongly agree	31	50.00	50.00	100
	Total	62	100	100	

Based on the data, half of the respondents (50%) strongly agree that international organizations should be involved in improving the cyber security of the Nigerian telecommunication industry. A very small percentage of the respondents (3.23%) disagree with this idea. There are no respondents who are undecided on this matter. Overall, most respondents believe that international organizations have a role to play in improving the cyber security of the Nigerian telecommunication industry. While independent research of its own, the ongoing global economic crisis, amongst other reasons, supports the need to solicit the help of INGOs.

Table 16. Do you think ethical hackers should be regulated in the Nigerian telecommunication industry?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	3	4.8	4.8	4.8
	Disagree	2	3.2	3.2	8.0
	Undecided	13	21.0	21.0	29.0
	Agree	10	16.1	16.1	45.1
	Strongly Agree	34	54.8	54.8	100.0
	Total	62	100.0	100.0	100.0

The survey results show that most 62 respondents (54.8%) believe ethical hackers should be regulated in the Nigerian telecommunication industry. A small minority of respondents (8%) disagreed or strongly disagreed with the idea. The remaining respondents (29%) were undecided. This finding indicates that most respondents view the regulation of ethical hackers as necessary for ensuring security and privacy in the telecommunication industry. By regulating ethical hackers,

the industry can prevent unauthorized access to sensitive information and protect against cyber-attacks. It is important to note that the results are based on a limited sample and may not reflect the views of the entire population. Further research should be conducted to gain a more comprehensive understanding of the issue.

Table 17. Do you believe the Nigerian telecommunication industry is taking enough steps to prevent data breaches?

	n	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	10	16.1	16.1	16.1
	Disagree	15	24.2	24.2	40.3
	Undecided	20	32.3	32.3	72.6
	Agree	15	24.2	24.2	96.8
	Strongly agree	2	3.2	3.2	100
	Total	62	100	100	100

A significant percentage of the respondents in the Nigerian telecommunication industry (40.3%) disagree or strongly disagree that enough steps are being taken to prevent data breaches. 32.3% of the respondents still decide, indicating a lack of confidence or uncertainty about the industry's efforts to prevent data breaches. Only 24.2% of the respondents agree or strongly agree that the industry is taking enough steps to prevent data breaches. The results indicate that most respondents believe the Nigerian telecommunication industry needs to take more steps to prevent data breaches. This highlights the need for the industry to improve its efforts to ensure the security of its customers' data.

Table 18. The Nigerian telecommunication industry needs to prioritize the implementation of cyber security measures.

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly disagree	0	0	0	0
Disagree	0	0	0	0
Undecided	1	1.6	1.6	1.6
Agree	27	43.5	43.5	45.2

Valid	Strongly agree	34	54.8	54.8	100
	Total	62	100	100	100

The majority of the respondents in the Nigerian telecommunication industry (54.8%) strongly agree that cyber security measures should be prioritized. Only 1.6% of the respondents are undecided, implying that the rest have a clear issue. No respondents disagree or strongly disagree that cyber security measures should be prioritized, indicating a universal agreement among the industry. The results suggest that the Nigerian telecommunication industry should recognize the importance of cyber security measures and should prioritize their implementation.

Table 19. Ethical hacking practices effectively ensure the security of Nigeria's telecommunication industry.

		Frequency	Percent	Valid Percent	Cumulative Percent
	Strongly disagree	4	6.45%	6.45%	6.45%
	Disagree	11	17.74%	17.74%	24.29%

Valid	Undecided	7	11.29%	11.29%	35.58%
	Agree	9	14.52%	14.52%	50.10%
	Strongly agree	31	50.00%	50.00%	100.00%
	Total	62	100.00%	100.00%	

The table shows respondents' opinions on the effectiveness of ethical hacking practices in ensuring the security of the telecommunication industry in Nigeria. Out of 62 respondents, 31 (50%) strongly agreed that ethical hacking practices are effective in ensuring the security of the telecommunication industry in Nigeria, 9 (14.52%) agreed, 7 (11.29%) were undecided, 11 (17.74%) disagreed, and 4 (6.45%) strongly disagreed. These findings imply that most respondents believe that ethical hacking practices are effective in ensuring the security of the telecommunication industry in Nigeria. This suggests that the telecommunication industry in Nigeria could benefit from adopting and implementing ethical hacking practices to improve its security measures.

Table 20. Companies in the Nigerian telecommunication industry should invest more in the training and development of their cyber security personnel.

	n	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	0	0%	0%	0%
	Disagree	0	0%	0%	0%
	Undecided	4	6.45%	6.45%	6.45%
	Agree	15	24.19%	24.19%	30.64%
	Strongly Agree	43	68.87%	68.87%	100%
	Total	62	100%	100%	100%

Based on the table above, out of 62 respondents, 43 (68.87%) strongly agree that companies in the Nigerian telecommunication industry should invest more in the training and development of their cyber security personnel. 15 (24.19%) agreed, while 4 (6.45%) were undecided. No respondents strongly disagreed or disagreed with this statement. Most of the respondents believe that investment in the training and development of cyber security personnel is crucial for companies in

the Nigerian telecommunication industry. This highlights the importance of having trained and skilled personnel to protect against cyber threats and ensure the security of sensitive information. Companies that ignore this need may face the consequences such as data breaches and loss of customer trust.

Table 21. The government of Nigeria should take more concrete steps to regulate the telecommunication industry to protect sensitive data.

	N	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	0	0%	0%	0%
	Disagree	0	0%	0%	0%
	Undecided	2	3.23%	3.23%	3.23%
	Agree	18	29.03%	29.03%	32.26%
	Strongly agree	42	67.74%	67.74%	100%
	Total	62	100%	100%	

Out of 62 participants, 67.74% strongly agree that the government of Nigeria should take more concrete steps to regulate the telecommunication industry to protect sensitive data. 29.03% of the participants agree with this statement, 3.23% are undecided, and 0% strongly disagree. The results show that most participants believe that Nigeria's government needs to take stronger measures to regulate the telecommunication industry to protect sensitive data. This highlights the importance of ensuring the security of personal information and the need for the government to take active steps to prevent any potential breaches or violations.

Table 22. The current cyber security measures implemented by the telecommunication industry in Nigeria are sufficient to mitigate cyber threats.

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly disagree	37	60.32%	60.32%	60.32%
Disagree	18	29.03%	29.03%	89.35%
Undecided	0	0%	0%	89.35%
Agree	3	4.84%	4.84%	94.19%
Strongly agree	4	6.45%	6.45%	100.00%

Valid	Total	62	100.00%	100.00%	100.00%

The table above shows the survey results on the current cyber security measures implemented by the telecommunication industry in Nigeria. Based on the results, 60.32% of the participants strongly disagreed with the statement, while 29.03% disagreed. Only 4.84% of the participants agreed with the statement, and 6.45% strongly agreed. These results imply that most participants believe that more than the current cyber security measures in the telecommunication industry in Nigeria is needed to mitigate cyber threats. This suggests that the industry needs improvement and enhancement of cyber security measures to better protect against cyber-attacks and prevent data breaches.

CHAPTER FIVE

5.0 Discussion

The Nigerian telecommunications industry has experienced tremendous growth in recent years, with increased subscribers and the adoption of new technologies. However, with this growth comes 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 cyber-attacks. 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 a recent 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.

In line with the findings of previous studies (Tettey et al., 2016; Akujuobi et al., 2018), the results of this study suggest that cyber security should be considered a critical component of the Nigerian telecommunications industry. To ensure the continued growth and success of the industry, measures must be taken to enhance the security of sensitive information and assets. This includes

the implementation of ethical hacking and cyber security measures and developing a workforce with the necessary skills and knowledge to address the evolving nature of cyber threats.

A recent study explored the current state of ethical hacking and cyber security in the Nigerian telecommunications industry and found that many companies face significant challenges. For example, the study found that many companies need more resources and expertise to effectively address cybersecurity issues, including a shortage of trained personnel and inadequate funding for cybersecurity solutions (Adeyemo, 2020). Additionally, the study revealed that many companies are not fully aware of the extent of the cyber security risks that they face and may not be fully prepared to respond to a cyber-attack (Adeyemo, 2020)

Another challenge Nigerian telecommunications companies face is the rapid pace of technological change. With the increasing use of new technologies, such as cloud computing, the internet of things (IoT), and big data, the industry is exposed to new and complex security risks that must be addressed (Adeyemo, 2020). These new technologies have the potential to transform the industry. Still, they also create new cybersecurity challenges that must be addressed to protect sensitive information and assets. A recent study explored the current state of ethical hacking and cyber security in the Nigerian telecommunications industry. The findings provide important insights into the challenges faced by the industry and the need for additional solutions to address these challenges.

The study found that Nigeria's telecommunications industry faces several cybersecurity challenges, including a lack of trained personnel, inadequate funding, and insufficient investment in cybersecurity solutions (Adeyemo, 2020). Additionally, the study revealed that the increasing use of digital technologies, such as cloud computing, the internet of things (IoT), and big data, has

created new and complex security risks that need to be addressed (Adeyemo, 2020). One of the study's key findings was the need for increased investment in ethical hacking and cyber security solutions. According to Adeyemo (2020), companies must invest more in cyber security solutions, including firewalls, intrusion detection systems, and encryption technologies, to prevent cyber-attacks and protect sensitive information and assets. This is especially important for the telecommunications industry, given its critical role in supporting national security and economic growth.

In conclusion, the study's findings highlight the importance of companies in the Nigerian telecommunications industry taking proactive measures to address the challenges of ethical hacking and cyber security. This includes increased investment in cyber security solutions, employee training and education, and partnerships with government agencies. By addressing these challenges, companies in the industry can protect sensitive information and assets and continue to support the growth and development of the Nigerian telecommunications industry. The study also found that companies in the Nigerian telecommunications industry need to increase their focus on ethical hacking and cyber security training and education. This includes training for employees on how to recognize and respond to cyber threats, as well as training for ethical hackers on detecting and preventing cyber-attacks (Adeyemo, 2020).

In terms of the limitations of the study, it is important to note that the findings may be representative of only some of the telecommunications industry in Nigeria, as the sample size was relatively small and limited to a specific geographic location. Additionally, the study relied on self-reported data from participants, which may have introduced some bias to the results.

Conclusively, the findings of this study highlight the need for increased investment in ethical hacking and cyber security solutions in the Nigerian telecommunications industry, as well as the importance of training and education, partnerships with government agencies, and ongoing efforts to address cybersecurity challenges. Future research could explore these issues in greater depth and examine the impact of cybersecurity solutions on the overall performance and competitiveness of the Nigerian telecommunications industry.

5.1 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 programs, and developing a cyber security workforce with the necessary skills and knowledge to address the evolving nature of cyber threats.

5.2 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

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

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.

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.

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.

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

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.

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.

Ewepu G, (2016) Nigeria loses N127bn annually to cyber-crime — NSA available at:http://www.vanguardngr.com/2016/04/nigeria-loses n127bn-annually-cyber-crime-nsa/Retrieved Jun. 9, 2016.

Eduproject. (n.d.). ETHICAL HACKING AND CYBER SECURITY IN NIGERIAN TELECOMMUNICATION INDUSTRY: ISSUES AND SOLUTIONS COMPUTER SCIENCE Project Topics. RESEARCH PROJECT TOPICS AND PROJECT TOPICS ON EDUCATION. Retrieved May 7, 2023, from https://eduproject.com.ng/computer-science-education/ethical-hacking-and-cyber-security-in-nigerian-telecommunication-industry-issues-and-solutions/index.html

Fitzgerald, J. (2018). Firewalls and Network Security. In Introduction to Network Security (pp. 49-71). Springer.

Ibrahim, M. A., Yusuf, A. B., Saidu, A. S., & Ahmad, M. S. (2018). Cybersecurity challenges in Nigeria: The way forward. In Proceedings of the 2nd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2017 (pp. 147-157). Springer. doi: 10.1007/978-981-10-7288-0_14

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.

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.

Laura, A. (1995): Cyber Crime and National Security: The Role of the Penal and Procedural Law",Research Fellow, Nigerian Institute of Advanced Legal Studies., Retrieved from http://nials-nigeria.org/pub/lauraani.pdf

Major General G. G UMO (2010): Cyber Threats: Implications For Nigeria's National Interest, Retrieved from https://docs.google.com/file/d/0B9sby6N v5O3M2 FlNWIzZj gtMDRiO S00Nj I1LThmMj ItNmI0Nzg5 NGVlNTM2/edit?num=50&sort=name&layout=list &pli=1

Odeyemi, T. O., & Odeyinka, H. A. (2019). Cybersecurity challenges in Nigeria's telecommunications industry. Journal of Engineering and Applied Sciences, 14(20), 8404-8408. doi: 10.36478/jeasci.2019.8404.8408

Ogbuabor, J. E., Eze, U. C., & Uwazie, I. U. (2020). Cybersecurity threats and vulnerabilities in the Nigerian telecommunication industry: An exploratory study. In Proceedings of the 3rd International Conference on Computing, Mathematics and Statistics (pp. 94-100). Springer.

Ogunrinde, O. D., Oladele, A. S., & Ayo, C. K. (2020). An Analysis of the Nigerian Telecommunications Industry: A Review of Its Evolution, Challenges, and Future Prospects. Sustainability, 12(5), 1909.

Ogwezzy, U. (2018). Cybersecurity and Ethical Hacking: Challenges and Prospects for Nigeria's Economic Growth. International Journal of Computer Science and Information Security, 16(8), 51-56.

Okereke, F. N., Njoku, C. G., & Ezugwu, I. U. (2020). Ethical hacking in Nigerian telecommunications industry: A panacea for cyber security challenges. International Journal of Scientific and Research Publications, 10(8), 189-193.

Oliver, E.O.(2010): Being Lecture Delivered at DBI/George Mason Univeristy conference on Cyber security holding, Department of Information Management Technology, Federal Univerity of Technology, Owerri, Nov. 1-2

Otu, E. N., Nwachukwu, I. N., Nweke, E. N., & Ugwuanyi, C. C. (2021). Cyber Security and the Nigerian Telecommunications Industry: Challenges and Solutions. International Journal of Cyber Criminology, 15(1), 117-136.

Oyebanjo, O. J., & Oyebisi, I. (2019). Cybersecurity and data privacy regulation in Nigeria: A critical review. African Journal of Science, Technology, Innovation and Development, 11(3), 285-292.

Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. 12 (2). ISSN 1558-7215.

Tunji, A. (2022, October 21). Cyber Warfare and Physical Damage – the War without Ammunitions. Security Outlines. Retrieved July 9, 2023, from https://www.securityoutlines.cz/cyber-warfare-and-physical-damage-the-war-without-ammunitions/

Vladimir, G.(2005), International Cooperation in Fighting Cyber Crime. http://www.crime-research.org/articles/

Kianpour, Mazaher; Kowalski, Stewart; Øverby, Harald (2021). "Systematically Understanding Cybersecurity Economics: A Survey". Sustainability. 13 (24): 13677. doi:10.3390/su132413677

Worldometer. (n.d.). Population by Country (2023). Worldometer. Retrieved July 9, 2023, from https://www.worldometers.info/world-population/population-by-country/