World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Research Article)

Ethical Hacking and Cybersecurity in the Nigerian Telecommunication Industry

Blessing Ngozi Eze [1, *], Daniel Taiwo Jemiri [2], Obed Ocholofu Jeremiah [3], Okoi Michael Obeten [4] and Adeyanju Idowu Quasim [5]

[1] The Department of Computer and Robotics Education, Faculty of Vocational and Technical Education, University of Nigeria Nsukka, Nigeria.
[2] The Department of Computer Science, School of Information and Communication Technology, Federal University of Technology Owerri, Nigeria.
[3] The Department of Mathematics and Computer Science, Faculty of Science, Reverend Father Moses Orshio Adasu University, Nigeria.
[4] The Department of Computer Science, School of Information and Communication Technology, Auchi Polytechnic, Nigeria.
[5] The Department of Computer Science, Faculty of Computing and Information Technology, Osun State University, Nigeria.

World Journal of Advanced Research and Reviews, 2026, 29(02), 061-065

Publication history: Received on 18 December 2025; revised on 30 January 2026; accepted on 02 February 2026

Article DOI: https://doi.org/10.30574/wjarr.2026.29.2.0273

Abstract

This study examined "Ethical Hacking and Cyber security In Nigerian Telecommunication Industry". Methodology: Relevant data were drawn from secondary sources of data such as online journals, textbooks, in which content analysis was used to analyze the data. The result of the findings revealed that ethical hacking plays an important role in controlling cybercrime in telecommunication sector. The study concluded that Overall, ethical hacking is very necessary to keep the cyber defense system strong in the Nigerian telecommunication industry. The demand for security steps taking in advance has turned very urgent since the cyber threats continue evolving in their complexity and frequency. Through vulnerability tests and mock attacks, ethical hackers allow the telecom providers to unveil the security weaknesses and fix them before the hackers' intervention is done. Such a step in the defense protects not only the customer's most sensitive data and the network, but also builds up the trust of the users in the services provided by the digital networks Finally the study recommends that The government, through regulatory agencies such as the Nigerian Communications Commission (NCC), should come up with such policies that are practically implementable as well as leading to the encouragement of the use of ethical hacking as a preventive measure instead of responding to breaches after they have taken place. There is also the need for a greater level of cooperation amongst telecom companies, cybersecurity experts, academic institutions, and law enforcement agencies to create a more robust and skill-driven cybersecurity workforce. The continuous training and certification schemes should be made available to cover the existing skills gap and also to ensure that the practice of ethical hacking is at par with the global standards. As a result of such a preemptive and well-coordinated maneuver, the Nigerian telecommunication sector can not only greatly diminish its exposure to cyber thrusts, but also garner increased public trust in its digital infrastructure.

Keywords: Ethical Hacking; Cyber security; Nigerian Telecommunication Industry

1. Introduction

One of the significant achievements of the internet in the business world is that virtually any data handling activity such as sorting, coding, modifying, and generating reports both customized and generic in a real-time processing mode has become easier for individuals, companies, industries, and even governments and not-for-profit organizations. On the other hand, it has greatly contributed to the occurrence of unexpected side effects such as criminal activities, spamming, credit card fraud, ATM fraud, phishing, identity theft, and the creation of a thriving enclave for cybercriminals to execute

[*] Corresponding author: Blessing Ngozi Eze

their nefarious activities (Ali, Khan & Ahmad 2021). One of the repercussions of the internet that made people feel uneasy and have mixed feelings of admiration and terror was the immoral usage of the net by cyberspace users to commit crimes. This issue has recently become more complex and phenomenal, thus requiring a rapid response in the form of rules which would protect the internet and its users. A cyber murder incident that was the first-ever scenario of such a case in history occurred in the United States seven years ago. Crime in a simple description is doing something unlawful which is punishable by the government or by some other authority. In spite of the differences among various criminal law systems and the absence of a universal definition of crime, a few legal characterizations have also been mentioned for this issue.

Cybercrime refers to the commission of unlawful acts in, on, or through the internet which aim at tricking, cheating, or causing harm to a network device like a computer, phone, or any other device. Cybercrime is such that the operations of a computer network or device are forcibly stopped or disrupted using malicious software (malicious code), a computer virus, or a denial-of-service attack (DOS). Perpetrators can use innocent victims to commit more crimes.

One of the things that have a big positive impact on the telecommunication sector is ethical hacking, which is basically internet security in Nigeria. The well-being of Nigeria both security-wise and economically largely relies on escalated cyber security as well as the safeguarding of the country information infrastructure (Ali, Khan & Ahmad 2021). Making the web more secure (and protecting Internet users) is now at the core of the whole process of service development and governmental policy.

Just like the fraudsters, ethical hackers use the same testing and bypassing methods to access the system. However, they do not exploit the vulnerabilities found, but instead, they reveal them and provide suggestions on how to fix them, which enables the enterprise to raise the overall security (Ali, Khan & Ahmad 2021). The activity has grown to be a significant sub-industry of the information security sector and has broadened to include the security of the organization's physical and human aspects. Even if a test has been passed, it does not always imply that the network or system is entirely secure. However, the system should be able to resist such automated attacks as a test is essentially a security check. Prevention of cybercrime undoubtedly needs to take the place of the national strategy for cybersecurity and the safeguarding of vital information infrastructures. Legal provisions that prohibit the illicit use of information and communication technology (ICT) and wicked acts that threaten the security of essential national infrastructures are the ones that should be enacted in particular here, such as passing legislation (European Commission 2020).

To properly prevent, plan, react, and recuperate from calamities, the government agencies, the business community, as well as the citizens, has to cooperate. It reverts to them being jointly responsible for it at a national level. In Nigeria telecommunication sub-sector, the rate of cybercrime has gone viral and it has been rising exponentially for the past couple of years. The negative consequences for the country socio-economic position are very frightening.

The development has been made more complicated and unusual in a very short time, and this fact alone has demanded a reaction in the next day in a form of rules that would safeguard both users and the net. Data prove that there is always a cybercrime somewhere in the world every day since 2008. It is quite evident that Nigerians have just started to realize the full potential of the internet. Serial crimes that the country used to be little known for have now been heavily dominated by telephony-enabled frauds.

Before 2001, when MTN started its operations in Nigeria, the cybercrime phenomenon had no global links to Nigeria. Over time, the country is being associated with various kinds of crimes, among which financial crimes that were facilitated by the use of telecommunication services. Victims find themselves increasingly more susceptible and, to some extent, more innocent, with respect to the possibilities that these tricksters opened for them. This research is primarily an overview of ethical hacking and information security in the telecommunications sector in Nigeria. It is to this the study centers on Ethical Hacking and Cybersecurity In Nigerian Telecommunication Industry.

2. Methodology

This research has been done by qualitative analysis method. Some literature like newspapers, textbooks, journals and other and ethical hacking and cybersecurity in Nigerian Telecommunications Industry related written materials were considered for the study. The study is mainly based on secondary data.

3. Data presentation and analysis

3.1. Research question I: To what extent does cybercrime impact on the performance of telecommunication industry in Nigeria?

One of the major impacts of telecommunication in Nigeria that are going to be felt in the long range is cybercrime which undermines operational efficiency, financial stability, customer trust, and regulatory compliance. The ubiquity of cyber threats like data breaches, SIM swap fraud, ransomware attacks, and service disruptions has escalated the risks for telecom operators and users alike. These evil acts usually result in the absence of normal function of the network, which is direct service delivery and hence customer satisfaction will be lowered, and the industry performance will be weakened.

On the financial side, the money to fight cybercrime in the Nigerian telecom sector is enormous. To deal with the constantly changing threat landscape, organizations will have to spend a lot of money on cybersecurity infrastructure, the training of staff, and the setting up of compliance mechanisms. Besides, the company may lose huge amounts of money because of fraud and cyberattacks, not only because the thieves take their assets but also due to the exit of customers and reputational harm. Trust among customers will be lost if telecom operators are seen as incapable of securing the data and privacy of consumers. Loyalty towards customers will weaken resulting in lower revenues and market competitiveness.

Besides that, the growing intricacy of cyber threats also impedes innovation and the adoption of new technologies such as 5G and the Internet of Things (IoT), which are dependent on the provision of a safe digital environment. In Nigeria where the telecom industry is the main driver of the digital transformation and the country economic growth, the continuous cyber threats are constituting a big challenge to the progress of the industry. The Nigerian Communications Commission (NCC) as a regulator has come up with guidelines and policies to handle these risks, however, the problem of large gaps in enforcement and technical capabilities still exists. Fundamentally, cybercrime is a major barrier to the excellent performance of the telecommunications industry in Nigeria.

3.2. Research Question II: What are the causes of cybercrime and its impact on the telecommunication industry?

According to Obi (2017) Cybercrime in the telecom sector has been fueled by a mix of technological, organizational, economic, and human factors. The increase in the digitization and interconnectivity of telecom networks is one of the major reasons.

In general, service providers in less developed countries like Nigeria may not have enough money, qualified personnel, or organizational willingness to put into practice strong security frameworks. Technical assistance (TA) which is needed to help train, recruit, and retain talented IT security staff is limited and does not keep pace with the rapid growth of the telecommunications market in Nigeria. Lack of strict regulatory leadership and poor collaboration between government, private sector, and international partners are also key factors in the increasing prevalence of cybercrime.

Human factors are the major considerations in a list of internal threats, social engineering, and negligent users besides which are no less important. Workers who are either a part of the company or a third-party vendor are the ones who have access to some straight sensitive systems. In such cases, they may directly or indirectly cause the security to be breached. Besides, phishing attacks and identity theft as a few of the methods criminals use to get unauthorized access to networks and user accounts.

The telecommunication industry is suffering from cybercrime to a very high degree, and the effects are diverse. Among the most immediate consequences are financial losses that result from direct theft, fraud, and the cost of remediation activities. The service disruptions that might be caused by these kinds of attacks as Distributed Denial of Service (DDoS) may lead to downtime, which will affect the users to the extent of thousands of them and cause a drop in consumer confidence. These kinds of disruptions make the reputation of telecom providers lose their value and maybe regulatory penalties or legal liabilities are right to instruction them.

In addition, data breaches related to customer information are the sources of significantly negative consequences such as legal worries and brand damage. When betrayal of trust takes place, the customer base will most probably turn to competitors and the firm will lose not only market share but also revenue. The presence of cybercrime acts as a deterrent to the innovation of new products as companies become more conservative and less willing to venture into the adoption of new technologies if they are not given proper security assurance.

3.3. Research question III: What are the benefits of ethical hacking and its impact on the telecommunication industry in Nigeria?

Ethical hacking, or penetration testing, as well as the use of white-hat techniques, can be considered important factors of the general security system improvement in telecommunication. In Nigeria, as the telecom sector is not only thriving but also getting more and more vulnerable to the attacks of cybercriminals, ethical hacking has become an indispensable instrument for pinpointing the weaknesses, waiting for the bad guys to exploit them (Kumar & Tripathi 2022).

One of the major advantages of ethical hacking is that it brings in power proactive threat detection. It is by acting as real-world hackers that ethical hackers let telecom companies find the weakest spots in their systems, for instance, old software, weak encryption, wrongly set network devices. Consequently, the operators will fix the security holes before the thieves exploit them and thus lower the danger of service distortions, data leaks, and money loss.

On top of this, ethical hacking can also bring compliance and regulatory readiness. The telecommunications firms will find themselves under immense pressure from the likes of the Nigerian Communications Commission (NCC) concerning their cybersecurity standards. They will be able to utilize ethical hacking as part of their risk assessment and compliance audit activity. This goes a step further in showing the exercise of due diligence and also the meeting of both the national and international standards of cybersecurity, for example, GDPR and ISO 27001.

Last but not least, customer data and privacy receive a new layer of security as a result of ethical hacking. As the telecom sector is highly reliant on data, the practice of ethical hacking is indispensable to ensure that critical customer information such as call records, personal ID, and financial data is stored and transmitted in a secure way. Apart from drastically decreasing the odds of data breaches, this also gives consumer trust and brand credibility, two points of extreme importance in the race of the market for the same customer base (Kumar & Tripathi 2022).

In addition to that, ethical hacking forms the foundation for capacity building by creating the need for more cybersecurity professionals in Nigeria. More telecom companies will need the services of ethical hackers thus more local professionals will be trained and the country will be less reliant on foreign consultants. The benefits of ethical hacking in the telecommunication sector in Nigeria cannot be overstated. It not only makes network security stronger but also avoids cyber-attacks that could cost a lot, ensures regulatory compliance, gives security to consumer data, and encourages innovation. As the nature of cyber threats continues to change, the use of ethical hacking techniques is not merely a technical task but a strategic requirement for the creation of a secure and sustainable telecommunications sector in Nigeria.

4. Discussion of findings

i) This finding matches with the study by Obi, Isioma Ruby (2017), which used qualitative, interview-based empirical research to examine the role of government in Nigeria mobile telecommunications industry with a focus on cybercrime. By talking to 18 people who work in the field, ranging from NCC officials to telecom operators, the study outlines how poor governance that is less than fully funded and weak implementation of policy have a negative impact on the performance of the telecom sector and its ability to bounce back ii) This finding is consistent with the empirical work by Philip (2024) "Cybercrime and the Challenges of Socio-Economic Development in Nigeria". The empirical study locates the main sources of cybercrime as being the lack of jobs, poverty, and the vulnerabilities of the technology and further explains how these lead to a decline in the visibility of the country, less foreign investment, and reduced telecommunication infrastructure reliability iii) In the end, the results that research are consistent with research by Akinyemi, Adetunji Akinfemiwa (2023) Ethical Hacking and Cyber Security in Nigeria Telecommunication Industry: Issues and Solution. The diploma thesis utilizes a descriptive and inferential research design, with the data being collected through a self-administered questionnaire addressed to 62 professionals working in the telecommunication industry in Nigeria. The study discloses that although the industry is facing difficult situations such as a shortage of technical expertise, limited budget allocations, and weak cybersecurity policies, it is still able to identify the importance of ethical hacking.

5. Conclusion

Overall, ethical hacking is very necessary to keep the cyber defense system strong in the Nigerian telecommunication industry. The demand for security steps taking in advance has turned very urgent since the cyber threats continue evolving in their complexity and frequency. Through vulnerability tests and mock attacks, ethical hackers allow the telecom providers to unveil the security weaknesses and fix them before the hackers' intervention is done. Such a step in the defense protects not only the customer's most sensitive data and the network, but also builds up the trust of the users in the services provided by the digital networks.

In Nigeria, the use of ethical hacking contributes to the overall network strength, compliance with regulations, and improved reliability of the services, as the telecommunications sector is the pillar of the digital transformation. The value of ethical hacking is becoming more and more apparent with the gradually overcoming of the difficulties such as lack of skilled personnel, poor cybersecurity strategies, and limited resources. The industry needs to keep investing in the tools for ethical hacking, the training and the enforcement of policies, thus, it will be essential for the security of Nigeria's telecommunications against the new cyber threats and for digital economy to grow sustainably.

Recommendation

It is important that there be an intentional and consistent effort to have ethical hacking as part of the fundamental security strategy of the telecom operators, if the aim is to have more detailed ethical hacking and cybersecurity in the Nigerian telecommunication organizations. Accordingly, Telecom operators must build a culture where they continuously assess their vulnerabilities, collaborate with hackers who are putting their skills and knowledge into practice, and invest in tools that facilitate penetration testing. Hired ethical hackers who are equipped with the skills to foresee, and therefore, disarm, the threats before they get out of hand, are a must.

The government, through regulatory agencies such as the Nigerian Communications Commission (NCC), should come up with such policies that are practically implementable as well as leading to the encouragement of the use of ethical hacking as a preventive measure instead of responding to breaches after they have taken place. There is also the need for a greater level of cooperation amongst telecom companies, cybersecurity experts, academic institutions, and law enforcement agencies to create a more robust and skill-driven cybersecurity workforce. The continuous training and certification schemes should be made available to cover the existing skills gap and also to ensure that the practice of ethical hacking is at par with the global standards. As a result of such a preemptive and well-coordinated maneuver, the Nigerian telecommunication sector can not only greatly diminish its exposure to cyber thrusts, but also garner increased public trust in its digital infrastructure.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Akinyemi, A. A. (2023). Ethical hacking and cyber security in Nigeria telecommunication industry: Issues and solution (Diploma thesis). Charles University, Faculty of Social Sciences. ([CU Digital Repository][1])

[2] Ali, R., Khan, S., & Ahmad, M. (2021). Artificial intelligence in telecom cybersecurity: Trends and future directions. Journal of Network and Computer Applications ,184, 103093. https://doi.org/10.1016/j.jnca.2021.103093

[3] European Commission. (2020). General Data Protection Regulation (GDPR). https://gdpr.eu/

[4] Kumar, N., & Tripathi, R. (2022). Securing 5G networks: A comprehensive cybersecurity strategy. IEEE Communications Surveys & Tutorials, 24 (2), 1012–1035. [https://doi.org/10.1109/COMST.2022.3154398](https://doi.org/10.1109/COMST.2022.3154398

[5] Obi, I. R. (2017). The role of government in the Nigerian mobile telecommunications industry: A focus on cybercrime and mobile broadband policies (Unpublished master's thesis). University of the Witwatersrand.

[6] Philip, S. F. (2024). Cybercrime and the challenges of socio-economic development in Nigeria: Implications for telecommunications. [Title adapted for clarity]. \[Journal/Publication]. ([ResearchGate][3])