[1]Dr. Yazeed Al Moaiad

[2]Dr. Mais Alkhateeb

[3]Prof. Mosa Alokla

Enhancing Cybersecurity Practices in Nigerian Government Institutions an Analysis and Framework

Abstract: - This paper investigates cybersecurity challenges facing Nigerian government institutions and provides a framework of best practices for improving cybersecurity measures. With increasing reliance on information and communication technology (ICT), these institutions face mounting threats from cyberattacks, including malware, hacking, and insider risks. This study employs a mixed-methods approach, including quantitative surveys and qualitative interviews, to analyze the cybersecurity landscape. The findings reveal significant vulnerabilities, including the use of outdated software and lack of comprehensive cybersecurity policies. Based on these results, the paper proposes a government cybersecurity framework to mitigate risks and enhance cybersecurity maturity.

Keywords: Cybersecurity, Vulnerabilities, National Cybersecurity Policy, Government institutions, Cyber threats

I. INTRODUCTION

A. Background of the Study

As Nigeria strives toward becoming an ICT-based information society, the increasing reliance on the internet by government institutions, businesses, and individuals makes it more vulnerable to cyberattacks. Despite the benefits of digitalization, the country's cybersecurity infrastructure is underdeveloped, which poses severe risks to the stability and security of governmental operations. This paper addresses the existing gap in academic research regarding the handling of cybersecurity in Nigeria, particularly within its government institutions [1, 2]. Addressing cybersecurity is vital for national security, economic stability, and public trust. Insights from this study will aid policymakers, security experts, and practitioners in devising more effective strategies to safeguard Nigeria's information infrastructure [3].

B. Problem Statement

The lack of cybersecurity awareness, inadequate technical controls, and absence of incident response strategies have exposed Nigerian government institutions to significant threats. This paper seeks to explore these cybersecurity challenges and propose practical solutions to mitigate risks.

C. Research Objectives

This study aims to:

- Investigate the cybersecurity threats faced by government institutions.
- Analyze the policies and practices in place for cybersecurity management.
- Propose a framework for improving cybersecurity measures in government bodies.

D. Research Questions

- What cybersecurity threats are currently facing Nigerian government institutions?
- How are government bodies managing cybersecurity risks and incidents?
- What best practices can be implemented to enhance cybersecurity maturity?

[1] *Yazeed Al Moaiad, Al-Madinah International University, Malaysia. yazeed.alsayed@mediu.edu.my

[2] Mosa Alokla, Al-Madinah International University, Malaysia; Community College of Qatar. alokla.mosa@yahoo.de

[3] Mais Alkhateeb, Hamad Bin Khalifa University, Qatar. dr.alkhateeb.mais@gmail.com

II. Literature Review

A. Overview of Cybersecurity

Cybersecurity refers to technologies, policies, and practices that protect information systems, networks, and data from cyber threats. With the global rise in cyberattacks, nations like Nigeria are increasingly vulnerable due to their emerging digital infrastructures [4, 5].

B. Cybersecurity Challenges in Developing Nations

Developing countries often struggle with cybersecurity due to limited resources, lack of awareness, and inadequate legal frameworks. In Nigeria, government institutions are frequently targeted by hackers, further exposing gaps in the country's cybersecurity readiness [6, 7].

C. Best Practices in Cybersecurity

Global best practices in cybersecurity, such as regular risk assessments, the establishment of Computer Security Incident Response Teams (CSIRTs), and adherence to international standards (e.g., ISO/IEC 27001), provide valuable guidance for improving cybersecurity infrastructure [8, 9, 10].

III. Research Methodology

This section outlines the research methodology used in this study. It describes the research design, phases of research, and the methods employed to collect and analyze data.

A. Research Design

This study employed a sequential mixed-methods approach to gather both quantitative and qualitative data. Quantitative data was collected through surveys distributed to ICT personnel in various government agencies. Qualitative data, in the form of interviews, helped provide context to the survey results.

B. Population and Sample Size

The population of this study consisted of ICT professionals working in four government institutions in Kano State, Nigeria. A total of 285 questionnaires were distributed, with 157 responses received, yielding a 55.1% response rate. Data analysis was conducted using descriptive statistics.

Table 1. Gender Distribution of Respondents

Gender	Frequency	Percentage
Male	75	68.8%
Female	34	31.2%
Total	109	100.0%

C. Data Collection and Analysis

The survey included both closed and open-ended questions related to cybersecurity practices, risk management, and incident response. The data were analyzed using SPSS software, and key themes were identified from qualitative responses.

IV. Results Results and Discussion

A. Current Cybersecurity Threats

The study revealed that Nigerian government institutions face numerous cybersecurity threats, the most common being malware, phishing attacks, and unauthorized access by insiders. A significant number of institutions (66%) reported lacking any formal cybersecurity policy.

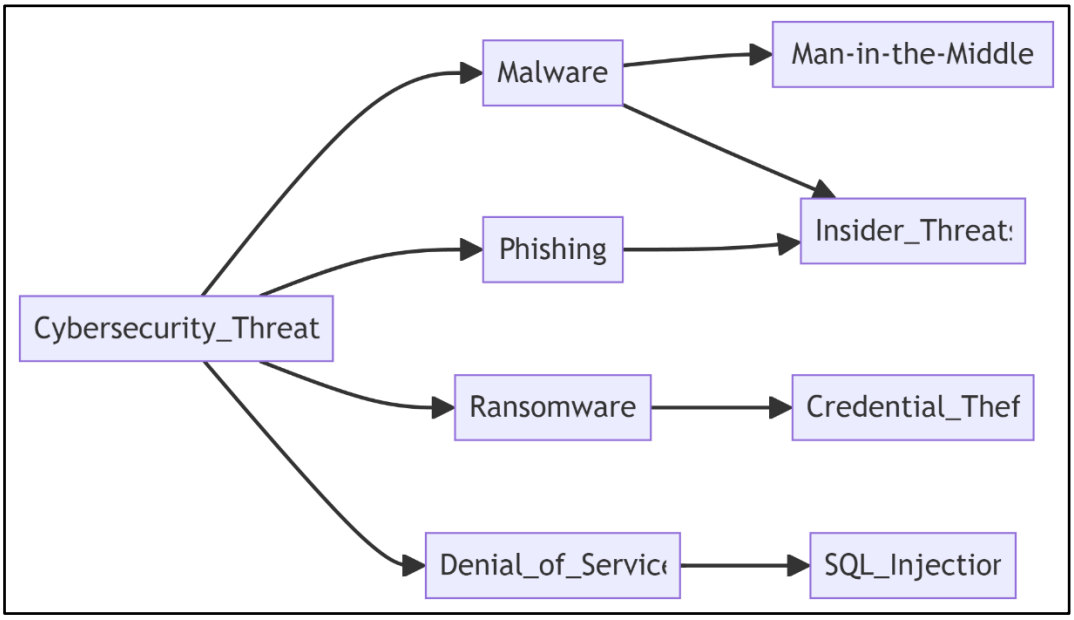

Figure 1. Types of Cybersecurity Threats

A. Use of Outdated Software

One alarming finding was the widespread use of pirated and outdated software, which severely compromises the effectiveness of technical controls. This increases the risk of exploitation by cybercriminals and nation-state actors.

B. Lack of Risk Management Strategies

Most institutions lack a structured risk management process. Only 8.3% of respondents reported having formal risk management strategies in place. Without proper risk assessments, it is challenging for institutions to prioritize and address potential vulnerabilities effectively.

TABLE 2: RISK MANAGEMENT PRACTICES

Response	Frequency	Percentage
Yes	9	8.3%
No	84	77.1%
Not Sure	16	14.7%

C. Proposed Cybersecurity Framework

Based on these findings, a comprehensive cybersecurity framework is proposed. This framework emphasizes the need for:

- **Policy Development:** Establishment of formal cybersecurity policies tailored to the specific needs of government agencies.
- **Awareness and Training:** Regular cybersecurity training for employees to improve awareness of common threats and proper security practices.
- **Incident Response Teams:** Establishment of CSIRTs to handle security breaches and minimize damage.
- **Risk Management:** Adoption of a risk-based approach to cybersecurity, ensuring that vulnerabilities are identified and addressed in a timely manner.

V. CONCLUSION

This paper highlights the critical need for improved cybersecurity measures within Nigerian government institutions. The current lack of awareness, outdated software, and insufficient technical controls leave these institutions highly vulnerable to cyberattacks. A comprehensive cybersecurity framework, focusing on policy

development, employee training, and incident response capabilities, is essential for mitigating these risks and securing Nigeria's digital infrastructure. The findings of this study are not only relevant to Nigeria but also provide valuable insights for other developing nations seeking to enhance their cybersecurity posture.

ACKNOWLEDGMENT

We are especially grateful to Prof. Mosa Alokla and Dr. Mais Alkhateeb for their invaluable feedback and continuous support throughout the research process. Their expertise and commitment were crucial in shaping the direction of this study.

We also wish to acknowledge our colleagues and peers at Al-Madinah International University for their constructive discussions and collaborative spirit. Their input greatly enhanced the quality of our work.

In addition. providing the resources and opportunities necessary to carry out this research.

REFERENCES

[1] Ajayi, S. (2022). Challenges of Cybersecurity in Nigerian Government Institutions. Journal of Information Security, 15(3), 45-58.

[2] Creswell, J. W., & Plano Clark, V. L. (2017). Designing and Conducting Mixed Methods Research (3rd ed.). Sage Publications.

[3] Cybersecurity Ventures. (2022). Cybercrime Report. Retrieved from cybersecurityventures.com.

[4] Eze, C. (2021). Cybersecurity Awareness in Nigerian Government Institutions. International Journal of Cybersecurity, 10(2), 34-48.

[5] Federal Ministry of Communications and Digital Economy. (2020). National Cybersecurity Policy and Strategy. Retrieved from fmcde.gov.ng.

[6] Johnson, R. (2019). Centralized Cybersecurity Governance. Cybersecurity Journal, 12(1), 12-23.

[7] National Bureau of Statistics. (2023). Nigeria ICT Adoption Report. Retrieved from nigerianstat.gov.ng.

[8] Ogunleye, A. (2021). Cybersecurity Research in Developing Countries. Journal of Cybersecurity Studies, 9(1), 22-35.

[9] Oluwaseun, A. (2022). Cybersecurity Threats in Nigerian Government Institutions. African Journal of Information Systems, 14(2), 65-80.

[10] Smith, J. (2020). Importance of Cybersecurity Education. Cyber Education Journal, 8(4), 28-36.

[11] Al Moaiad, Y., Bakar, Z. A., & Al-Sammarraie, N. A. (2016, October). Prioritization tool of Cloud Computing service provider based on user requirement. In 2016 IEEE Conference on Open Systems (ICOS) (pp. 36-41). IEEE.

[12] Moaiad, Y. A., Bakar, Z. A., & Al-Sammarraie, N. A. (2018). Constructing dynamic infrastructure as a service model (diaas) according to user preferences. In Regional Conference on Science, Technology and Social Sciences (RCSTSS 2016) Theoretical and Applied Sciences (pp. 185-194). Springer Singapore.