CYBER SECURITY THREATS AND DIGITAL GOVERNANCE IN NIGERIAN BUSINESSES

PRESENTED

BY

Jeremiah Theophilus Nwaguiyi: jerry.nwaguiyi@federalpolyoko.edu.ng, 08068869864

Raymond Ezeh: **vulcanrayjude@gmail.com,** 07062835796

Onyebuchi Christopher Okoye: okoyeonyebuchi808@gmail.com 07037223702

TO

THE

INTERNATIONAL JOURNAL OF APPLIED SCIENCE RESEARCH FEDERAL POLYTECHNIC, OKO ANAMBRA STATE, NIGERIA

SCHOOL OF APPLIED SCIENCE AND TECHNOLOGY

FEDERAL POLYTECHNIC, OKO

ABSTRACT

As Nigerian businesses increasingly embrace digital transformation in different areas, they face growing challenges from cyber security threats. This paper examines the intersection of cyber security threats and digital governance in Nigerian businesses across all sectors, highlighting the critical importance of robust digital governance frameworks in mitigating cyber risks. Through an analysis of the current state of digital governance in Nigeria, the paper explores the challenges and opportunities for enhancing cyber security and offers recommendations for businesses and policymakers.

Five Keywords: Cybersecurity Threats, Digital Governance, Data Protection, Nigerian Businesses, Cybercrime Prevention

INTRODUCTION

1.1 BACKGROUND OF THE STUDY

The rapid adoption of digital technologies by businesses in Nigeria has brought about significant benefits, including improved efficiency, innovation, and global competitiveness. However, this digital transformation has also exposed businesses to a wide range of cyber security threats, from malware and ransomware attacks to data breaches and phishing scams. As these threats continue to evolve in complexity and frequency, the need for effective digital governance has become paramount.

1.2 RESEARCH OBJECTIVES

This paper aims to explore the relationship between cyber security threats and digital governance in Nigerian businesses. Specifically, it seeks to:

- Identify common cyber security threats faced by Nigerian businesses.
- Assess the current state of digital governance in Nigerian businesses.
- Analyze how digital governance frameworks can mitigate cyber security threats.
- Provide recommendations for strengthening cyber security through improved digital governance.

1.3 SCOPE AND LIMITATIONS

The study focuses on Nigerian businesses across various sectors, examining both large enterprises and small to medium-sized enterprises (SMEs). While the paper provides a broad overview of the challenges and opportunities in digital governance, it does not delve into specific technical solutions or industry-specific case studies.

1.4 SIGNIFICANCE OF THE STUDY

Safeguarding Private Information: Nigerian companies are becoming more and more dependent on digital channels, which leaves them open to cyberattacks. By addressing cybersecurity risks, fraud and data breaches are avoided and sensitive consumer and financial data is protected.

Regulation Compliance: In order for Nigerian firms to abide by national and international cybersecurity laws and regulations (such as the GDPR for businesses that conduct business internationally and the Nigeria Cybercrimes Act 2015), digital governance is crucial.

Increasing Trust and Reputation: Consumers, investors, and stakeholders are more trusting of businesses that implement robust cybersecurity measures and efficient digital governance. Businesses are more likely to obtain a competitive edge if they manage data securely and openly.

LITERATURE REVIEW AND THEORY

2.0 **OVERVIEW OF CYBER THREATS**

Cyber security threats are defined as malicious activities that target an organization's information systems with the intent to steal, disrupt, or damage digital assets. Common threats include:

Phishing: Deceptive attempts to obtain sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity.

Malware and Ransomware: Malicious software designed to gain unauthorized access to systems, often holding data hostage until a ransom is paid.

Data Breaches: Unauthorized access to confidential information, leading to data theft or leakage.

Denial-of-Service (DoS) Attacks: Overwhelming a system with traffic to render it inoperable.

2.1 **PREVALENCE AND IMPACT**

Nigerian businesses have increasingly become targets for cyber criminals, given the growing digital landscape and relatively weak cyber defenses. According to recent reports, Nigeria ranks high in the number of cyber attacks in Africa, with businesses suffering significant financial losses, reputational damage, and operational disruptions. Akinrolabu, O., & Oyeleke, O. (2020).

2.2 **FACTORS CONTRIBUTING TO VULNERABILITY**

Several factors contribute to the vulnerability of Nigerian businesses to cyber threats:

Outdated Technology: Many businesses operate on outdated or unsupported software, making them easy targets for cyber attacks.

Lack of Awareness: There is a general lack of cyber security awareness among employees and business leaders, leading to poor security practices.

Inadequate Governance: Weak digital governance structures result in inconsistent or inadequate security measures across organizations.

2.3. **DIGITAL GOVERNANCE IN NIGERIAN BUSINESSES**

Digital governance refers to the policies, frameworks, and processes that organizations implement to manage their digital assets, ensure compliance, and protect against cyber security threats. Omodunbi, B. A., Odiase, P. O., Olaniyan, M. O., & Esan, A. O. (2016). Effective digital

governance is essential for safeguarding sensitive information, maintaining regulatory compliance, and building customer trust.

2.4 **COMPONENTS OF EFFECTIVE DIGITAL GOVERNANCE**

Effective digital governance encompasses several key components:

Cyber Security Policies: Clearly defined policies that outline the organization's approach to managing cyber risks.

Compliance Frameworks: Adherence to national and international regulations related to data protection and cyber security.

Incident Response Plans: Preparedness for potential cyber attacks, including protocols for detection, response, and recovery.

Employee Training: Regular training programs to educate employees on cyber security best practices.

2.5 **CURRENT STATE OF DIGITAL GOVERNANCE IN NIGERIA**

While some Nigerian businesses have begun to implement digital governance frameworks, many still lack comprehensive strategies to manage cyber risks. Ayeni, F. (2019). Challenges such as limited resources, regulatory gaps, and a shortage of skilled cyber security professionals hinder the widespread adoption of effective digital governance.

2.6 **INTERRELATIONSHIP BETWEEN CYBER SECURITY THREATS AND DIGITAL GOVERNANCE**

Weak digital governance can exacerbate cyber security risks by creating gaps in protection and response mechanisms. Ndukwe, C., & Etim, C. (2022). Without clear policies and protocols, businesses are more likely to fall victim to cyber attacks, as they lack the necessary controls to prevent, detect, and mitigate threats.

2.7 **ROLE OF STRONG DIGITAL GOVERNANCE IN MITIGATING THREATS**

Adegboye, S., & Aderonke, A. (2021). Conversely, robust digital governance can significantly reduce the likelihood and impact of cyber threats. By implementing strong cyber security policies, conducting regular risk assessments, and fostering a culture of security awareness, businesses can better protect their digital assets and respond more effectively to incidents.

2.8 **CHALLENGES AND OPPORTUNITIES IN ENHANCING CYBER SECURITY AND DIGITAL GOVERNANCE**

CHALLENGES

Abubakar, M., & Haruna, B. (2018). Despite the recognized importance of digital governance, Nigerian businesses face several challenges in its implementation:

Regulatory Challenges: The absence of clear and enforceable regulations on cyber security hinders businesses from adopting standardized practices.

Financial Constraints: Limited budgets, especially among SMEs, restrict investments in advanced cyber security technologies and training.

Shortage of Expertise: The lack of skilled cyber security professionals in Nigeria makes it difficult for businesses to build and maintain effective digital governance structures.

OPPORTUNITIES

There are also significant opportunities to enhance digital governance and cyber security in Nigeria:

Public-Private Partnerships: Collaboration between the government and private sector can lead to the development of more comprehensive regulatory frameworks and the sharing of resources.

Technological Innovation: Advances in technology, such as artificial intelligence and blockchain, offer new tools for improving cyber security and digital governance. Chinedu-Eze, V. C., & Emmanuel, O. (2020).

Awareness Campaigns: Increased efforts to raise awareness about the importance of cyber security can drive better practices among businesses and employees.

2.9 FUTURE DIRECTIONS AND RECOMMENDATIONS

EMERGING TRENDS

As cyber threats continue to evolve, Olufuye, T. A. (2019). Nigerian businesses must stay ahead by adopting emerging trends in cyber security and digital governance:

AI and Machine Learning: Leveraging AI to detect and respond to cyber threats in real-time.

Blockchain Technology: Using blockchain for secure transactions and data integrity.

Regulatory Developments: Anticipating and preparing for new regulations that may impact digital governance practices.

SECTION 3

3.0 **RECOMMENDATIONS AND COCLUSION**

To strengthen cyber security and digital governance, Nigerian businesses should:

Develop Comprehensive Cyber Security Policies: Establish clear policies and procedures for managing cyber risks.

Invest in Employee Training: Regularly train employees on cyber security best practices and threat awareness.

Adopt Advanced Technologies: Utilize cutting-edge technologies to enhance security measures and stay ahead of cyber threats.

3.1 **POLICY RECOMMENDATIONS**

Policymakers should consider the following actions to support businesses in enhancing digital governance:

Establish Clear Regulatory Frameworks: Develop and enforce regulations that provide clear guidelines for cyber security and digital governance.

Promote Cyber Security Education: Invest in educational programs to build a pipeline of skilled cyber security professionals.

Encourage Collaboration: Foster public-private partnerships to share knowledge, resources, and best practices in digital governance.

3.2 **CONCLUSION**

As Nigerian businesses continue to navigate the complexities of digital transformation, the importance of robust digital governance cannot be overstated. By addressing the challenges and seizing the opportunities in digital governance, businesses can significantly enhance their cyber security posture, protect their digital assets, and build trust with customers and stakeholders. This paper has highlighted the critical need for Nigerian businesses to prioritize digital governance as a key strategy for mitigating cyber security threats, and has provided actionable recommendations for businesses and policymakers alike.

REFERENCES

Akinrolabu, O., & Oyeleke, O. (2020). Cybersecurity in Nigeria: An Overview of Threats and the Implementation of National Cybersecurity Strategies. Journal of Cyber Policy, 5(2), 223-238. https://doi.org/10.1080/23738871.2020.1764156

Omodunbi, B. A., Odiase, P. O., Olaniyan, M. O., & Esan, A. O. (2016). Cybercrimes in Nigeria: Analysis, Detection and Prevention. FUOYE Journal of Engineering and Technology, 1(1), 1-8.

Olufuye, T. A. (2019). Digital Transformation, Cybersecurity, and Data Protection in Nigerian Businesses. In: Proceedings of the Nigerian Computer Society Conference, 2, 45-57.

Abubakar, M., & Haruna, B. (2018). Cybersecurity Challenges and Adoption of Digital Governance in Nigeria: An Exploratory Analysis. International Journal of Information Systems and Change Management, 11(4), 328-343. https://doi.org/10.1504/IJISCM.2018.10019015

Adegboye, S., & Aderonke, A. (2021). The Impact of Cybersecurity Threats on Nigeria's Banking Sector: A Regulatory Perspective. Journal of Financial Crime, 28(3), 774-790. https://doi.org/10.1108/JFC-09-2020-0198

Ayeni, F. (2019). Challenges and Opportunities of Digital Governance in Nigeria's Public Sector. Nigerian Journal of Management Research, 8(2), 94-108.

Chinedu-Eze, V. C., & Emmanuel, O. (2020). The Role of Governance in Mitigating Cybersecurity Risks for Nigerian SMEs. Journal of Information Systems Management, 9(2), 62-78.

Ndukwe, C., & Etim, C. (2022). Exploring the Intersection of Cybersecurity and Digital Governance: A Nigerian Perspective. Journal of African Digital Policy, 3(4), 191-206.