09.30.2024 **JOURNAL OF**

African Sustainable Development (JASD) Vol. 5 No.2

DESIGNING A STRATEGIC FRAMEWORK FOR CYBER-SECURITY AWARENESS AND EDUCATION IN NIGERIA

***MOHAMMAD FAISAL; & **ALMUSTAPHA BELLO**

*Department of Computer Application, Integral University, Lucknow. **Integral University, India

Corresponding Author: mdfaisal@iul.ac.in

ABSTRACT

The proposed Cybersecurity Awareness and Education Framework presents a structured approach to enhancing cybersecurity knowledge across Nigeria. The framework is organized into five distinct layers and one overarching component, addressing different facets of cybersecurity education and awareness. The Strategic Layer outlines the national vision and policy for cybersecurity, while the Tactical Layer focuses on implementing actionable components such as the "B-iTech Nig" campaign and strategic partnerships. The Preparation Layer defines necessary resources and content, the Delivery Layer targets specific audience segments for effective education, and the Monitoring Layer emphasizes the evaluation and refinement of the initiative. The overarching component, Resources, encompasses the essential elements required for successful implementation, including personnel, information, infrastructure, and financial

Introduction

The rapid evolution of Information and Communication Technologies (ICTs) has profoundly transformed global communication, effectively erasing geographical barriers through the World Wide Web (Kritzinger & Von Solms, 2010). Despite these advancements, concerns about security in online communications and transactions remain significant (Kritzinger & Von Solms, 2010). As technological progress accelerates, so do the volume and sophistication of cyber-attacks, underscoring the need for robust protection of personal and business

E-ISSN 3026-8575 P-ISSN 3027-1266

capital. This framework aims to foster a robust cybersecurity culture in Nigeria by delivering tailored, effective, and sustainable awareness and education programs.

Keywords: Nigeria, cyber-security, cyber-security awareness and education, strategic

Information. This protection is crucial not only for individual security but also for national security. To address these challenges, a comprehensive national framework for cybersecurity is essential. This study aims to develop a broader, more inclusive cybersecurity framework for the nation. It is structured into five interrelated sections: the introduction and problem statement; a review of related literature; the research methodology; the proposed framework, including its analysis and validation; and finally, the conclusion.

Statement of the Problem

In Nigeria, the increasing affordability of mobile devices, smartphones, and data packages has significantly expanded internet access. As of the end of 2019, internet penetration in Nigeria reached 61.2%, marking a 62,939% increase in usage from 2000 to 2020 (Internet World Stats, 2020). While this digital expansion offers tremendous opportunities, it simultaneously exposes users to new risks as cyberspace becomes a platform for criminal activities, raising significant concerns.

Despite various policies and initiatives aimed at improving cybersecurity awareness and education, Nigeria continues to experience a troubling rise in cybercrime. For example, in 2018, cyber fraud resulted in a loss of ₦1.9 billion affecting over 25,043 bank customers. The Consumer Awareness and Financial Enlightenment Initiative (CAFEi) has projected that cybercrime could cause losses of up to $6 trillion by 2030, both within and outside Nigeria (Internet World Stats, 2020).

Given these challenges, it is crucial for all internet users to prioritize the protection of sensitive information from cyber threats. Effective cybersecurity awareness and education are essential for safeguarding users in the digital environment. This paper aims to address this issue by proposing a comprehensive cybersecurity awareness framework for the Nigerian

government, designed to foster a culture of cybersecurity among all internet users.

Review of Key Concepts

Cyber Awareness and Education

The concept Awareness refers to the state of being conscious of events and occurrences, and in the context of cybersecurity, it involves understanding and perceiving online risks and threats. According to Arwa (2019) and Bada et al. (2019), cybersecurity awareness encompasses all measures taken to enhance users' knowledge of cybersecurity, focusing on understanding online risks and responding appropriately. Zilka (2017) emphasizes that cybersecurity awareness involves increasing knowledge about online risks and safe practices, while Ngoqo and Flowerday (2015) describe it as understanding security threats, their mechanisms, and anticipating potential outcomes. Khan et al. (2011) highlight the user's responsibility in cybersecurity, defining awareness as understanding its importance and taking responsibility. Kruger and Kearney (2006) break it down into what users know (knowledge), think (attitude), and do (behavior) regarding cybersecurity.

Zwilling et al. (2020) point out a widespread lack of awareness about cyber risks, particularly concerning app usage and social networks. This issue is critical for Nigerian users, who predominantly access cyberspace via smartphones and mobile apps. As cybersecurity now extends beyond desktops to include smartphones and other internet-enabled devices, it is vital to address these vulnerabilities (Cybersecurity and Infrastructure Security Agency (CISA), 2019).

Education

Education is fundamental to raising awareness and fostering a cybersecurity culture. Venter et al. (2019) argue that cybersecurity education instills the need for precautions when engaging with cyberspace. Education equips users with the skills to recognize, identify, and mitigate online risks, thus playing a crucial role in developing cybersecurity behaviors. Tasevski (2016) contends that awareness and education are primary solutions for enhancing cybersafety, suggesting that many security breaches can be prevented with proper knowledge of cybercrimes and protective measures.

The lack of cybersecurity education has made African, and specifically Nigerian, users particularly vulnerable to cybercriminals. Providing education helps bridge

the gap in cybersecurity awareness, reducing successful cyber-attacks, increasing the likelihood of threat detection, and minimizing recovery times and losses (ngCERT, 2019). With global financial damage projected to reach $6 trillion by 2021 (CISCO, 2020), assessing and improving individual cybersecurity awareness and education is essential. This assessment should be a foundational step in developing effective cybersecurity strategies to prevent cybercrime and mitigate associated risks.

Nigeria's Cyber Awareness and Education Initiatives

The Nigerian government has recognized the growing dependence on cyberspace and the associated threats. This recognition has prompted efforts to address cyber threats, which have been exacerbated by inadequate cybersecurity awareness. This section reviews the various initiatives aimed at enhancing cyber awareness and education in Nigeria.

National Cybersecurity Initiative (NCI)

Established in 2003 in response to increasing cybercrime rates, the National Cybersecurity Initiative (NCI) was overseen by the Nigeria Cybercrime Working Group (NCWG). This group, composed of government officials, ICT ministries, and law enforcement agencies, aimed to promote public awareness about the dangers of cybercrime. Despite these efforts, the impact on awareness and education was limited. In 2006, the responsibilities of the NCWG were transferred to the Directorate of Cybersecurity (DOC) under the Office of the National Security Adviser (ONSA), yet significant public awareness and education gaps persisted (Ibikunle & Eweniyi, 2013; Maska, 2009).

National Cybersecurity Policy and Strategy

Launched in 2014 by the ONSA, the National Cybersecurity Policy (NCSP) aimed to combat rising cybercrime by enhancing public understanding and response to cyber threats (Osho & Onoja, 2015). The policy focused on national awareness, education, and advocacy through workshops, seminars, and media campaigns. However, evaluations of the strategy's implementation revealed shortcomings in monitoring and evaluation (ngCERT, 2017). The policy was updated in 2021 to address ongoing cybersecurity challenges and strengthen global collaborations (CTC, 2021). Despite these updates, cybercrime continues to escalate.

Nigeria Computer Emergency Response Team (ngCERT)

The Nigeria Computer Emergency Response Team (ngCERT), operating under the ONSA, manages cyber risks and coordinates incident response strategies. ngCERT plays a key role in providing security advisories, alerts, and general education to improve the cybersecurity posture of individuals and organizations in Nigeria (ngCERT, 2019).

National Cyber Security Awareness Month (NCSAM)

Launched in 2004 by the U.S. Department of Homeland Security (DHS) and the National Cyber Security Alliance (NCSA), National Cyber Security Awareness Month (NCSAM) is observed every October to promote online safety. Although the NCSAM originated in the U.S., it has been adopted by various countries. In Nigeria, while there has been no official declaration for October as Cybersecurity Awareness Month, agencies such as the National Information Technology Development Agency (NITDA), the National Identity Management Commission (NIMC), and the Nigerian Communications Commission (NCC) have embraced the initiative to raise public awareness and educate their staff (NCC, 2020).

One significant gap in the current cybersecurity awareness initiatives in Nigeria is their lack of practical application. Existing programs often fail to bring awareness directly to internet users in a manner that is actionable and relevant to their everyday experiences. There is a crucial need to move beyond theoretical knowledge and provide practical demonstrations on how to handle cyber threats effectively.

This paper proposes the development of cybersecurity awareness frameworks that address this gap by offering hands-on, practical guidance. By implementing frameworks that actively engage users and demonstrate real-life scenarios and responses, it aims to enhance the effectiveness of cybersecurity education and empower individuals to better protect themselves against cyber threats.

Research Methodology

This study proposes an All-Inclusive Cybersecurity Awareness and Education Framework, developed using the design science research paradigm. Design science research involves creating new or modified artifacts to address specific problems and evaluating their effectiveness (Venable & Baskerville, 2012;

Dresch et al., 2015). This approach is guided by a structured process, as outlined by Peffers et al., which includes the following steps:

1. **Problem Identification and Motivation**: Define the problem and justify the need for a solution.
2. **Objectives of a Solution:** Derive the objectives based on the identified problem.
3. **Design and Development:** Create the solution as an artifact.
4. **Demonstration**: Show how the artifact effectively addresses the problem.
5. **Evaluation:** Assess how well the artifact solves the problem and measure its quality (Peffers et al., 2007; Hevner et al., 2004).
6. **Communication**: Disseminate findings through scholarly or professional publications.

Evaluation is crucial in design science research for validating the effectiveness of the artifact. In this study, elite/expert interviews were used for evaluation, as they provide insights from knowledgeable individuals about the problem and solution (Cooper et al., 2007; Marshall & Rossman, 2011). Access to experts was facilitated through email, aligning with modern communication practices. Two experts were selected based on their experience in cybersecurity and their contributions to cyber-awareness and education. Elite one is a cybersecurity specialist at the National Identity Management Commission (NIMC) with extensive publications on national cybersecurity awareness. Elite two is the Research Group Leader at the National Information Technology Development Agency (NITDA), with significant research and presentations in cybersecurity. Feedback from these experts was used to refine the framework, as detailed in Section Four of this study.

The Cybersecurity Awareness and Education Framework

This section introduces the proposed Cybersecurity Awareness and Education Framework, which is structured into five distinct layers and one overarching component, as follows:

1. The Strategic Layer
2. The Tactical Layer
3. The Preparation Layer

4. The Delivery Layer
5. The Monitoring Layer
6. Resources (as the overarching component)

Each layer represents a key theme in the framework, which is visually summarized in Figure 1. The following subsections will provide a detailed overview of each layer.

The Strategic Layer

The Strategic Layer embodies the government's overarching vision for cybersecurity awareness and education. This vision, as outlined in Nigeria's draft Cybersecurity Policy, aims to cultivate a robust cybersecurity culture. This layer is composed of three key components:

i. National Cybersecurity Policy: This document outlines the country's primary objectives for enhancing cybersecurity awareness and education.
ii. Responsible Unit: This refers to the dedicated administration tasked with overseeing cybersecurity awareness and education efforts. The framework suggests three potential approaches for establishing this unit:
   - ✓ Creating a new administration specifically for cybersecurity.
   - ✓ Utilizing existing government departments.
   - ✓ Delegating responsibilities to a private organization.
iii. Strategic Plan: Once the responsible unit is established, a comprehensive strategic plan should be developed. This plan will define the approach Nigeria should take to advance cybersecurity awareness and education.

The Tactical Layer

The Tactical Layer builds upon the strategic vision outlined in the Strategic Layer and focuses on actionable components to advance cybersecurity awareness and education. This layer includes four main components:

i. National Cybersecurity Awareness and Education Campaign: Proposed as "B-iTech Nig" (Basic Informative Technology for Nigerians), this campaign will serve as a comprehensive initiative encompassing all sub-campaigns and programs.
ii. Partnerships: Establishing collaborations with public and private sectors, academia, and international entities is crucial. These

partnerships will enhance the campaign's effectiveness by integrating diverse expertise and fostering global alignment in cybersecurity awareness. Academia will contribute research to tailor the campaign to Nigerian needs.

iii. Sub-Campaign Activities: B-iTech Nig will deploy various sub-campaigns to engage different segments of the population and these includes:

- ✓ **B-iTech Week:** An annual event aimed at raising awareness about cybersecurity as a shared responsibility and promoting current practices and issues.
- ✓ **B-iTech Community Outreach:** A program encouraging community involvement through volunteering to spread cybersecurity awareness.
- ✓ **B-iTech For All:** An inclusive website offering up-to-date cybersecurity information for the general public, covering topics like cyber-bullying, identity theft, fraud, and online security.
- ✓ **B-iTech For Schools:** Aimed at integrating cybersecurity into school curricula and delivering age-appropriate education to primary and secondary students.

The effectiveness of these sub-campaigns hinges on addressing the following questions:

- ✓ What specific topics should B-iTech Nig cover?
- ✓ What communication tools should be utilized?

These questions will be explored further in the subsequent sections of the framework.

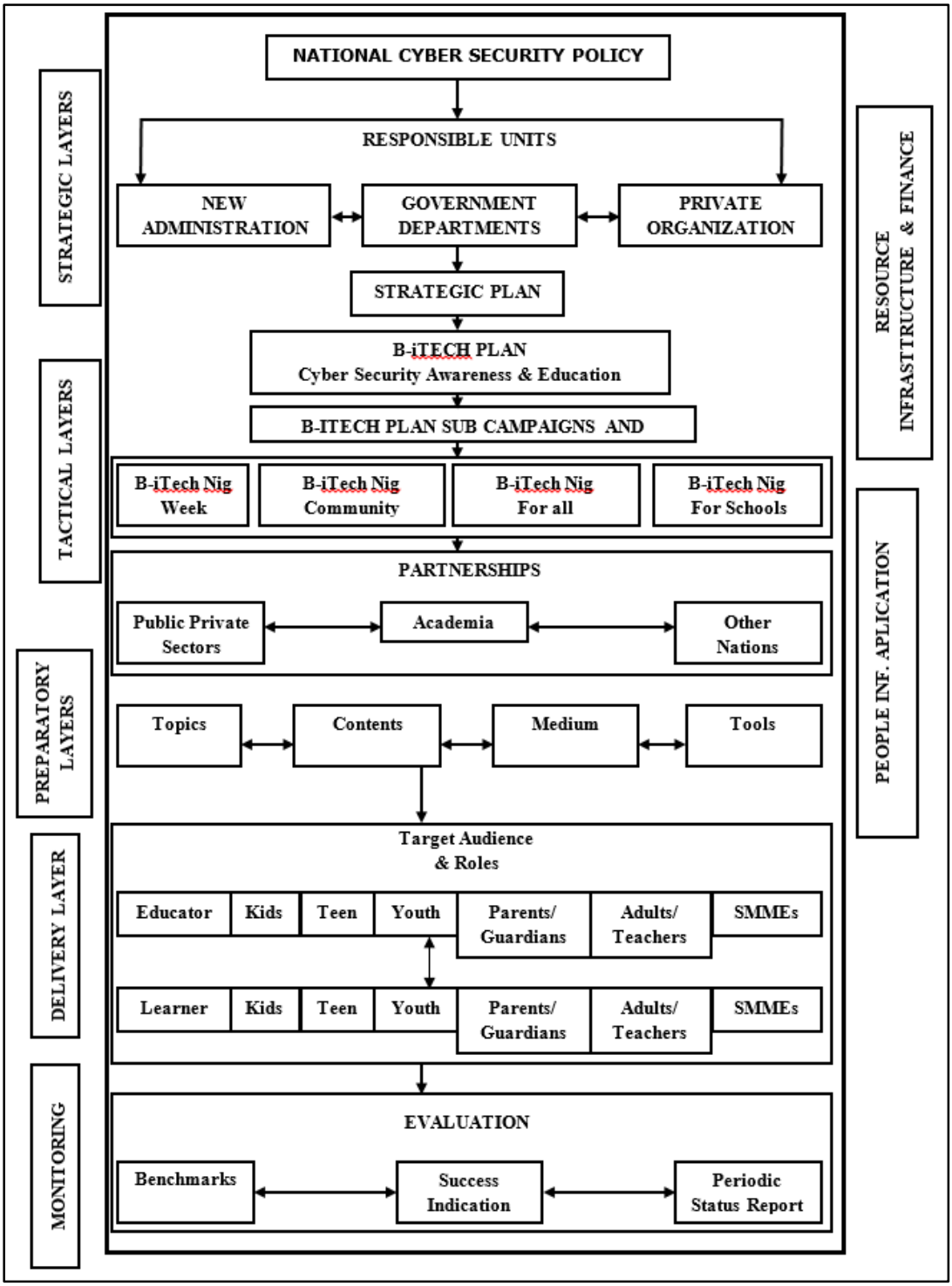
The Preparation Layer

The Preparation Layer defines the resources and materials needed for the B-iTech Nig campaign. It includes four components:

- ✓ Topics: Identified topics for the campaign include cyber-bullying, cyber-stalking, identity theft, fraud, phishing, online privacy, and secure behavior. These topics address common cybersecurity issues and are essential for comprehensive awareness.

E-ISSN 3026-8575 P-ISSN 3027-1266

B-ITECH NIG" (BASIC INFORMATIVE TECHNOLOGY FOR NIGERIANS)



CYBER SECURITY AWARENESS AND EDUCATION FRAMEWORK

E-ISSN 3026-8575 P-ISSN 3027-1266

- ✓ Content: The content should be tailored to the target audience. For instance, content on cyber-bullying for children might include guidance on reporting incidents, while for parents, it might focus on recognizing signs of cyberbullying.
- ✓ Medium: The choice of medium—whether paper-based or electronic—should align with the content and target audience. For example, electronic mediums might include websites and videos, whereas paper-based materials could involve brochures and flyers.
- ✓ Tools: Tools for delivering the content include websites, videos, games, quizzes, etc. The selection of tools should match the topic, content, and medium to ensure effective delivery of information.

The Preparation Layer aims to address the following question:

- ✓ To which target audiences should B-iTech Nig deliver cybersecurity awareness and education?

This question will be answered in the next section, ensuring that the framework is effectively tailored to reach and educate various segments of the Nigerian population.

The Delivery Layer

The Delivery Layer focuses on targeting specific audience segments for the B-iTech Nig initiative and defining their roles. The proposed target audiences include:

a) Children under 13 years
b) Teenagers
c) Youths
d) Parents/Guardians
e) Adults
f) Teachers
g) Small, Medium, and Micro-sized Enterprises (SMMEs)

Each audience will have dual roles: Learner and Educator. As learners, they will utilize the resources provided by B-iTech Nig to enhance their cybersecurity knowledge. As educators, they will share their newfound knowledge within their communities, promoting broader awareness. The effectiveness of the framework

will be assessed based on the clarity and engagement of these roles and the impact on each target audience.

The Monitoring Layer

The Monitoring Layer is critical for evaluating the effectiveness of the cybersecurity awareness and education efforts. Key activities include:

- ✓ Establishing Benchmarks: Defining clear benchmarks to measure progress.
- ✓ Defining Success Indicators: Identifying specific indicators to evaluate success.
- ✓ Generating Periodic Reports: Producing regular reports to assess the status of the campaign.

Feedback from these evaluations will be used to refine the B-iTech Nig campaign. For instance, if certain benchmarks or success indicators are not met, adjustments may be made to the Preparation Layer, such as revising topics, content, or tools.

Resources

The effective implementation of the framework requires several key resources:

a) People: Skilled individuals to execute various functions.
b) Information: Data and software needed for operation.
c) Infrastructure: Physical equipment, such as computers and servers.
d) Financial Capital: Funding necessary for the initiative's execution.

These resources, adapted from the Information Technology Infrastructure Library (ITIL), are essential for delivering a robust cybersecurity awareness and education program. The government must ensure these resources are adequately provided to support the framework's successful implementation.

Conclusion:

The Cybersecurity Awareness and Education Framework provides a comprehensive, multi-layered approach to bolstering cybersecurity knowledge and practices in Nigeria. By integrating strategic planning with tactical execution and robust monitoring, the framework ensures that cybersecurity awareness efforts are both systematic and adaptive. The delineation of distinct layers from the strategic vision and campaign development to targeted audience engagement

and resource management creates a cohesive strategy for advancing national cybersecurity resilience. The effectiveness of the framework will be continuously assessed through established benchmarks and success indicators, allowing for ongoing refinement and improvement. Ultimately, this structured approach aims to cultivate a widespread and enduring cybersecurity culture across Nigeria, empowering individuals and organizations to navigate and mitigate cybersecurity risks effectively.

Reference

Arwa, A.A (2019). Effectiveness of Cyber Security Awareness Program for young children: A Case Study in UAE. International Journal of Information Technology and Language Studies (IJITLS). Vol. 3, Issue. 2, (2019). pp. 8-29

Bada, M., Sasse, A.M., & Nurse, J.R.C. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? Arxiv. arXiv: 1901.02672.

CISA (2019). Security Tip (ST05-017): Cybersecurity for Electronic Devices. Internet: https://us-cert.cisa.gov/ncas/tips/ST05-017, Accessed 19/11/2020

CISCO Networking Academy (2020). Cybersecurity. CISCO. Internet: https://www.netacad.com/sites/default/files/cybersecurity_infographic.pdf?utm_source=student_newsletter&utm_medium=email&utm_campaign=cyber_month

Conti, J., A. and M. O'Neil (2007). Studying power: qualitative methods and the global elite". Qualitative Research, vol. 7, no. 1, pp. 63–82

Cooper, D., R., and Schindler, P. S (2003). Business research methods. McGraw-Hill/Irwin New York.

CTC (2021). National Cybersecurity Policy And Strategy 2021. Counter Terrorism Centre. Internet: https://ctc.gov.ng/national-cybersecurity-policy-and-strategy/ Accessed 25/2/2021

Hevner, A. R., March, S., T., Park, J. and Ram, S. (2004). Design science in information systems research. MIS quarterly, vol. 28, no. 1, pp. 75–105.

Ibikunle, F. and Eweniyi, O. (2013). Approach to cyber security issues in nigeria: Challenges and solution. International Journal of Cognitive Research in Science, Engineering and Education.

Internet World Stats (IWS) (2020). Africa 2020 Population and Internet Users Statistics. Internet: https://www.internetworldstats.com/stats1.htm, Accessed 11/10/2020

Kritzinger, E. and von Solms, A (2010). Cyber security for home users: A new way of protection through awareness enforcement". Computers & Security, vol. 29, no. 8, pp. 840–847.

Marshall, C., and and Rossman, G., B. (2011). Designing qualitative research. Sage, 5th ed. edn., 2011.

Maska, D. (2009). The contemporary software security landscape. IEEE Security & Privacy, 5(3), 75-77. https://doi.org/10.1109/MSP.2009.49

Mikecz, A. (2012). Interviewing elites addressing methodological issues". Qualitative inquiry, vol. 18, no. 6, pp. 482–493

NgCERT (2017). Action Plan for Implementation of the National Cybersecurity Strategy. Internet: https://www.cert.gov.ng/ngcert/resources/draft-action-planncss.pdf, Accessed 10/10/2020.

NgCERT (2019). Nigeria Computer Emergency Response Team. Internet: https://www.cert.gov.ng/, Accessed 10/10/2020.

Ngoqo, B. & Flowerday, S. (2015). Information Security Behaviour Profiling Framework (ISBPF) for student mobile phone users. Computers & Security. 53. 10.1016/j.cose.2015.05.011.

Odumesi, J.O. (2015). Approaches to Increase Public Awareness on Cybersecurity. African Journal of Computing & ICT, Vol 8. No. 4, Pp 143-152. December, 2015. ISSN 2006-1781

Osho, O. & Onoja, A. (2015). National Policy and Strategy of Nigeria: A Qualitative Analysis. International Journal of Cyber Criminology. 9. 973-5089. 10.5281/zenodo.22390

Peffers, K. Tuunanen, T., Rothenberger, M., A., and Chatterjee, S. (2007). A design science research methodology for information systems research". Journal of management information systems, vol. 24, no. 3, pp. 45–77.

Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security – what goes where? Information & Computer Security, 26(1), 2–9. https://doi.org/10.1108/ics-04-2017-0025

Zilka, G.C. (2017). Awareness of E-safety and Potential Online Dangers Among Children and Teenagers. Journal of Information Technology Education Research. Volume 16, 2017.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F. & Basim, H.N. (2020). Cyber Security Awareness, Knowledge and Behaviour: A Comparative Study. Journal of Comp. Info. Systems, 1-16. DOI: 10.1080/08874417.2020.1712269