ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL1024

Challenges and Strategies for Enhancing ICT Security in Public Institutions

Okafor Godwin
(Centre for Peace and Security Studies,
University of Port Harcourt, Nigeria.)

Dr. Martha O. Musa
(Department of Cybersecurity, Faculty of Computing,
University of Port Harcourt, Nigeria.)

Abstract:- This study explores the challenges faced by public institutions in implementing and maintaining effective ICT security controls, focusing on the University of Port Harcourt. By examining the perceptions of various stakeholders, including ICT administrators, staff, and students, the research identifies key issues related to confidentiality, integrity, and availability within the institution's ICT systems. The findings highlight significant areas for improvement, such as policy enforcement, training, and risk management. The article provides practical recommendations and strategies for public institutions to enhance their ICT security measures, ensuring alignment with the CIA Triad model and addressing emerging security threats. These insights are crucial for policymakers and ICT professionals aiming to strengthen the security posture of educational institutions.

Keywords:- *ICT Security, CIA Triad, Public Institutions, Cyber Security.*

I. INTRODUCTION

In the realm of Information and Communications Technology (ICT) security, the CIA Triad model plays a fundamental role in ensuring a robust security framework within organizations. The CIA Triad, which stands for Confidentiality, Integrity, and Availability, forms the cornerstone of information security practices (Mahadi et al., 2018). This model emphasizes the interconnectedness of these three principles to establish a secure IT infrastructure (Crihan et al., 2023).

The CIA Triad is essential for guiding information security policies and is crucial for the dependable operation of systems, particularly in smart energy systems and computer networks (Banik, 2024; Alhawi et al., 2019). It serves as a benchmark model for evaluating the security of information in organizations, encompassing physical, logical, and perceptual security aspects (Ngwenya & Ngoepe, 2020). Moreover, the CIA Triad is utilized to measure the security level of systems, ensuring that they meet acceptable security standards (Al-Haija & Alsulami, 2022).

In the context of ICT security, the CIA Triad is instrumental in addressing security concerns in various domains such as IoT environments, quantum networks, and substation automation systems (Mahmoud et al, 2021; Horálek et al, 2023). By adhering to the principles of confidentiality, integrity, and availability, organizations can enhance their security posture and mitigate risks associated with cyber threats (Żebrowski et al., 2022).

Furthermore, the CIA Triad is not only limited to traditional information security but also extends to areas like data security optimization in cloud storage and security requirements engineering (Sudarsa, 2024; Fabian et al., 2009). It provides a comprehensive framework for classifying data based on security requirements and aligning security measures with organizational objectives (Sudarsa, 2024).

II. LITERATURE REVIEW

This section provides an overview of existing research on ICT security in public institutions, focusing on the CIA Triad model's principles of confidentiality, integrity, and availability. The review highlights the importance of these principles in maintaining a secure ICT environment and identifies common challenges encountered in their implementation.

In (Iordache et al, 2022), the authors explore the potential benefits of introducing multi-factor authentication (MFA) using biometrics as a standard practice to enhance cyber security in public institutions. They argue that integrating biometric-based MFA can significantly bolster the security framework, reducing the risks associated with unauthorized access and data breaches. Additionally, the authors advocate for the widespread implementation of this solution in conjunction with a redesigned network architecture based on the Zero Trust Architecture (ZTA) approach. This comprehensive approach would enable a more granular and robust method for securing networks and data, ensuring that trust is never implicitly granted, and access controls are continuously verified. By combining biometric MFA and ZTA, public institutions can achieve a higher level of security resilience and protect sensitive information more effectively.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL1024

In (Semlambo et al, 2022), the authors concentrated on identifying information system security threats and vulnerabilities in public higher learning institutions in Tanzania, with a particular focus on the Institute of Accountancy Arusha (IAA). Through their research, they discovered that several key factors significantly impact the security of information systems at IAA. These factors include human elements, such as the behaviour and awareness of individuals using the systems; policy-related issues, which encompass the presence or absence of robust security policies and protocols; the work environment, which includes the physical and organizational conditions in which the information systems operate; and demographic factors, which may relate to the varying characteristics of the institution's population, such as age, education level, and technical proficiency. By identifying and understanding these factors, the study provides insights that could help in developing more effective strategies to enhance information system security in similar educational institutions.

In (Al-Shanfari et al, 2022). a comprehensive theoretical model was developed to assess public sector employees' Information Security Awareness (ISA) intentions and their subsequent information security behaviour, integrating Protection Motivation Theory (PMT), the Theory of Planned Behaviour (TPB), General Deterrence Theory (GDT), and Facilitating Conditions. PMT explains how perceived threat severity, vulnerability, protective behaviour efficacy, and self-efficacy motivate individuals to protect themselves. TPB examines how attitudes, subjective norms, and perceived behavioural control influence intentions and actions, while GDT posits that the fear of sanctions deters undesirable behaviour. Facilitating Conditions refer to environmental factors that ease certain behaviours. Combined, these theories and conditions provide a robust framework for understanding and predicting public sector employees' intentions to engage in secure information practices. This integrated model suggests that these elements together offer the most influential approach to enhancing information security behaviour, aiding organizations in developing effective strategies to foster a culture of security awareness and compliance.

In (Ogunode et al, 2021), authors explore the challenges faced by public higher institutions in Nigeria during the deployment of Information and Communication Technology (ICT) facilities amid the Covid-19 pandemic. They identify inadequate funding, insufficient ICT infrastructure, the high cost of internet services, and unstable internet connectivity as major obstacles. These issues hindered the institutions' ability to support online learning and communication effectively. To address these challenges, the authors recommend increasing funding to develop and maintain robust ICT infrastructure, reducing internet service costs to make them more affordable, and improving the stability and reliability of internet services. By implementing these measures, public higher institutions in Nigeria can enhance their ICT capabilities, better supporting remote learning and administrative functions during and beyond the pandemic.

In this paper, Yakasai (2022)the author discuss the on-going challenge of ICT (Information and Communication Technology) unavailability in certain public institutions located in rural areas, despite the widespread accessibility of these technologies in the modern world. They highlight that while urban and more developed regions have significantly benefited from advancements in ICT, rural areas often remain underserved. This disparity in access results from several factors, including insufficient infrastructure, limited financial resources, and a lack of technical expertise in these regions.

III. METHODOLOGY

This study employs a mixed-methods approach, integrating both quantitative and qualitative data collection techniques to comprehensively assess the effectiveness of ICT security controls at the University of Port Harcourt.

- *Quantitative Data Collection:*

A total of 200 questionnaires were distributed among various stakeholders at the University of Port Harcourt, including ICT administrators, staff, faculty members, and students. The questionnaires were designed to evaluate the participants' perceptions of the confidentiality, integrity, and availability controls implemented within the university's ICT infrastructure. The survey items were measured on a Likert scale to quantify the level of agreement or disagreement with statements related to ICT security practices and policies.

- *Qualitative Data Collection*

To complement the quantitative data, in-depth interviews were conducted with selected ICT administrators and staff. These interviews aimed to gain deeper insights into the perceived effectiveness of existing security controls and to identify specific challenges and areas for improvement. The qualitative data provided contextual understanding and nuanced perspectives that enriched the interpretation of the survey results.

IV. DATA ANALYSIS

The quantitative data from the questionnaires were analysed using descriptive and inferential statistics to identify trends, patterns, and significant differences in the perceptions of security controls. Mean scores and standard deviations were calculated for each survey item to provide a summary of the responses. Additionally, chi-square tests were performed to examine the relationships between different variables and to test the study's hypotheses.

The qualitative data from the interviews were analysed using thematic analysis. This involved coding the interview transcripts to identify recurring themes and patterns related to the effectiveness of ICT security measures, challenges faced, and suggested improvements. The integration of both quantitative and qualitative data provided a holistic view of the ICT security landscape at the University of Port Harcourt.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL1024

V. FINDINGS AND DISCUSSION

A. Perception of Confidentiality Controls

The analysis of the data regarding the perception of confidentiality controls at the University of Port Harcourt reveals insightful findings. The responses indicate a general awareness of confidentiality policies among the stakeholders, which is a positive aspect of the institution's ICT security framework. However, the data also highlight the necessity for enhanced training programs to further bolster the security posture of the university.

- *Awareness and Effectiveness*

The mean score for the awareness of confidentiality policies is relatively high, indicating that a significant proportion of respondents are informed about the existing policies. This is a crucial step towards ensuring that the policies are adhered to and that sensitive information is protected. Additionally, the mean score for the effectiveness of access control measures also reflects a positive perception, suggesting that the current measures in place are considered adequate by the majority of respondents.

- *Need for Improvement*

Despite these positive indicators, the variability in the responses points to areas where improvements can be made. Specifically, the standard deviations indicate that there are differing opinions on the effectiveness and comprehensiveness of the confidentiality controls. This variability suggests that while some stakeholders feel confident in the measures, others may have reservations or have experienced gaps in the system.

- *Training Programs*

One of the key areas identified for improvement is the training programs related to confidentiality controls. The data suggest that although there is awareness, the depth of understanding and the ability to effectively implement these controls may be lacking. Enhanced training programs can address this issue by providing stakeholders with the necessary skills and knowledge to handle and protect confidential information more effectively. Training can also help standardize the understanding and application of confidentiality measures across the institution, reducing variability in perceptions and ensuring a more uniform security posture.

B. Perception of Integrity Controls

The analysis of data regarding the perception of integrity controls at the University of Port Harcourt indicates a generally positive assessment of the current measures in place. Respondents perceive these controls as effective in ensuring data accuracy and safeguarding against unauthorized modifications. However, the variability in responses suggests that there are still areas that require attention to maintain data completeness and integrity consistently.

- *Effectiveness in Ensuring Data Accuracy*

The mean scores for the effectiveness of integrity controls reflect a consensus among respondents that the current measures are adequate in preserving data accuracy. This perception is critical as accurate data is foundational to the institution's operations and decision-making processes. Effective integrity controls ensure that data remains reliable and trustworthy, thereby supporting the university's academic and administrative functions.

- *Protection Against Unauthorized Modifications:*

Respondents also generally perceive the integrity controls as effective in protecting data from unauthorized modifications. This aspect of data integrity is crucial in preventing data corruption and maintaining the trustworthiness of the information within the institution. The positive perception in this area suggests that the existing measures are performing well in safeguarding data integrity against potential internal and external threats.

- *Variability in Responses*

Despite the positive perceptions, the analysis reveals variability in the responses. The standard deviations indicate that not all respondents share the same level of confidence in the integrity controls. This variability highlights the existence of perceived gaps or inconsistencies in the application or effectiveness of these controls across different areas or departments within the university.

- *Need for Further Enhancements*

The variability in responses underscores the need for further enhancements to the integrity controls to ensure consistent data completeness and protection. The university should consider conducting a thorough review of its integrity controls to identify specific areas where improvements can be made. This might include standardizing protocols, increasing monitoring and auditing activities, and ensuring that all departments adhere to the same high standards of data integrity.

C. Perception of Availability Controls

The analysis of data on the perception of availability controls at the University of Port Harcourt reveals that these controls are generally viewed positively in terms of ensuring system reliability and resource accessibility. However, there are identified areas where improvements are needed to further enhance the institution's ability to recover quickly from disruptions and ensure continuous availability of ICT resources.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL1024

- *System Reliability:*

  Respondents generally perceive the current availability controls as effective in maintaining high system reliability. The mean scores indicate that the majority of users find the systems to be dependable, with minimal downtime. Reliable systems are crucial for the smooth operation of academic and administrative activities, and positive feedback in this area suggests that the university has implemented effective measures to keep systems running consistently.

- *Resource Accessibility:*

  The data also suggests that the availability controls are effective in ensuring that users can access necessary resources without significant delays. This is reflected in the high mean scores for resource accessibility, indicating that students, faculty, and staff can depend on the ICT infrastructure to support their educational and administrative needs. Ensuring resource accessibility is necessary to maintaining productivity and facilitating the educational process.

- *Quick Recovery from Disruptions*

  While the overall perception of availability controls is positive, the analysis highlights some areas for improvement, particularly in the institution's ability to recover quickly from disruptions. The variability in responses, as indicated by the standard deviations, suggests that some users have experienced delays or challenges in accessing systems following outages or disruptions. Quick recovery mechanisms are essential to minimize the impact of such disruptions on the university's operations.

- *Areas for Improvement:*

  To address these gaps, the university should focus on enhancing its incident response mechanisms and disaster recovery plans. This could involve:

- *Regular Testing and Updates**:***

  Conducting regular tests of disaster recovery and incident response plans to ensure they are effective and up-to-date with current threats and technologies.

- *Training and Awareness*

  Providing comprehensive training to ICT staff and users on the protocols to follow during disruptions to ensure swift and coordinated responses.

- *Infrastructure Upgrades*

  Investing in robust infrastructure and technologies that support rapid recovery and redundancy, such as backup systems and failover solutions.

VI. SECURITY VULNERABILITIES

The study conducted at the University of Port Harcourt identifies several critical security vulnerabilities within its ICT infrastructure. These vulnerabilities pose significant risks to the confidentiality, integrity, and availability of the institution's data and systems. Key areas of concern include unauthorized access to data, unauthorized modifications, disruptions impacting system availability, visitor access to the network, and devices configured by private vendors.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL1024

- *Unauthorized Access to Data:*

One of the primary security vulnerabilities identified is the potential for unauthorized access to sensitive data. Despite having confidentiality controls in place, the analysis reveals that there are still gaps that could be exploited by malicious actors. This unauthorized access can lead to data breaches, compromising the privacy of students, staff, and faculty, and potentially resulting in financial and reputational damage to the institution.

- *Unauthorized Modifications:*

The study also highlights vulnerabilities related to unauthorized modifications of data. Integrity controls are designed to ensure that data remains accurate and unaltered by unauthorized parties. However, the variability in responses suggests that these controls are not uniformly effective. Unauthorized modifications can undermine the trustworthiness of the institution's data, leading to incorrect information being used in decision-making processes and academic activities.

- *Disruptions Impacting Availability:*

Another significant vulnerability identified is the potential for disruptions that could impact the availability of ICT systems. The ability to access necessary resources and maintain system uptime is crucial for the smooth functioning of the university's operations. The data indicates that while availability controls are generally perceived as effective, there are areas where the institution's ability to recover quickly from disruptions could be improved. These disruptions can stem from various sources, including cyber-attacks, technical failures, or natural disasters.

- *Visitor Access to the Network:*

The study points out specific risks associated with visitors connecting their devices to the university's network without consulting the ICT unit or department. This practice poses a substantial security risk, as unauthorized devices can introduce malware, create vulnerabilities, and bypass existing security measures. Proper protocols and controls need to be established to manage and monitor visitor access to the network, ensuring that all connections are secure and authorized.

- *Devices Configured by Private Vendors:*

Additionally, the study identifies security risks associated with network devices installed and configured by private vendors. These devices may not always comply with the university's security policies or be configured to the institution's standards. This lack of oversight can create security gaps, making the ICT infrastructure more susceptible to attacks and unauthorized access. Ensuring that all devices are thoroughly vetted and configured according to strict security guidelines is essential to mitigate these risks.

VII. RECOMMENDATIONS

Based on the findings, the paper proposes several strategies to enhance ICT security in public institutions:

- *Training and Awareness:*

Ensure all stakeholders are adequately trained and understand the importance of security policies and procedures.

- *Policy Enforcement:*

Implement robust mechanisms to monitor compliance and address violations effectively.

- *Regular Updates:*

Periodically review and update security policies and plans to address emerging threats and changing organizational needs.

- *Comprehensive Risk Management:*

Maintain a regularly updated ICT risk register and engage all stakeholders in the risk management process.

- *Disaster Recovery and Business Continuity:*

Strengthen communication and enforcement of disaster recovery and business continuity plans.

VIII. CONCLUSION

Ultimately, this study contributes valuable insights into the current state of ICT security in public institutions and offers practical recommendations for enhancing the effectiveness of security controls. The adoption of a holistic and adaptive security strategy, rooted in the principles of the CIA Triad, will be pivotal in navigating the evolving threat landscape and ensuring the integrity, confidentiality, and availability of critical information systems.

REFERENCES

[1]. Abu Al-Haija, Q., & Alsulami, A. A. (2022). Detection of fake replay attack signals on remote keyless controlled vehicles using pre-trained deep neural network. Electronics, 11(20), 3376.

[2]. Alhawi, O. M., Mustafa, M. A., & Cordiro, L. C. (2019, September). Finding security vulnerabilities in unmanned aerial vehicles using software verification. In 2019 International Workshop on Secure Internet of Things (SIOT) (pp. 1-9). IEEE.

[3]. Al-Shanfari, I., Warusia, Yassin., Nasser, Tabook., Roslan, Ismail., Anuar, Ismail. (2022). Determinants of Information Security Awareness and Behaviour Strategies in Public Sector Organizations among Employees. International Journal of Advanced Computer Science and Applications, doi: 10.14569/ijacsa.2022.0130855

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL1024

[4]. Bania, A., Iatrellis, O., & Samaras, N. (2023). Information Communication Technologies (ICTs) and Disaster Risk Management (DRM): Systematic Literature Review. In Conference on Sustainable Urban Mobility (pp. 1779-1794). Springer, Cham.
[5]. Banik, S., & Banik, T. (2024). Survey on Simulation and Vulnerability Testing in Smart Grid.
[6]. Crihan, G., Craciun, M., & Dumitriu, L. (2022). Hybrid methods of authentication in network security. The Annals of "Dunarea de Jos "University of Galati. Fascicle III, Electrotechnics, Electronics, Automatic Control, Informatics, 45(1), 7-7.
[7]. Fabian, B., Gürses, S., Heisel, M., Santen, T., & Schmidt, H. (2010). A comparison of security requirements engineering methods. Requirements engineering, 15, 7-40.
[8]. Horalek, J., & Sobeslav, V. (2023). Security Baseline for Substation Automation Systems. Sensors, 23(16), 7125.
[9]. Iordache, C. A., Dragomir, A. V., & Marian, C. V. (2022, November). Public institutions updated enhanced biometric security, zero trust architecture and multi-factor authentification. In 2022 International Symposium on Electronics and Telecommunications (ISETC) (pp. 1-4). IEEE.
[10]. Karuvade, S., & Sanders, B. C. (2021). Security for Quantum Networks. arXiv preprint arXiv:2109.14107.
[11]. Mahadi, N. A., Mohamed, M. A., Mohamad, A. I., Makhtar, M., Kadir, M. F. A., & Mamat, M. (2018). A survey of machine learning techniques for behavioral-based biometric user authentication. Recent Advances in Cryptography and Network Security, 43-59.
[12]. Ngwenya, M., & Ngoepe, M. (2020). A framework for data security, privacy, and trust in "consumer internet of things" assemblages in South Africa. Security and Privacy, 3(5), e122.
[13]. Ogunode, N. J., Somadina, O. I., & Olatunde-Aiyedun, T. G. (2021). Challenges and problems of deployment of ICT facilities by public higher institutions during Covid-19 in Nigeria. Ogunode, NJ, Okwelogu, IS & Olatunde-Aiyedun, TG (2021). Challenges and problems of deployment of ICT facilities by public higher institutions during Covid-19 in Nigeria. International Journal of Discoveries and Innovations in Applied Sciences, 1(4), 30-37.
[14]. Semlambo, A. A., Mfoi, D. M., & Sangula, Y. (2022). Information systems security threats and vulnerabilities: A case of the Institute of Accountancy Arusha (IAA). Journal of Computer and Communications, 10(11), 29-43.
[15]. Sudarsa, D., Rao, A. N., & Sivakumar, A. P. (2024). Data Security Optimization at Cloud Storage using Confidentiality-based Data Classification. International Journal of Advanced Computer Science & Applications, 15(5).
[16]. Yakasai, B. A. (2022). Introduction Of ICT To Reshape Public Institutions In Rural Areas. Farabi Journal of Social Sciences, 8(2), 74-78.
[17]. Żebrowski, P., Couce-Vieira, A., & Mancuso, A. (2022). A Bayesian framework for the analysis and optimal mitigation of cyber threats to cyber-physical systems. Risk Analysis, 42(10), 2275-2290.