IJAAR PUBLISHING®

Scholarly Journal of Science and Technology Research & Development | ISSN: **2955-0807**
Vol. 2, Issue 5 (May, 2023) | www.ijaar.org/sjstrd

Building a Cyber Smart Team: The Imperative for Polytechnics in Nigeria

Augustine N. Egere

Email: austinendudi@yahoo.com

Department of Computer Science, The Polytechnic Bali, Taraba State.

Abstract:

As Nigeria continues to witness rapid advancements in technology and increased internet penetration, the need for a skilled and knowledgeable workforce in cybersecurity becomes crucial. This article explores the imperative for polytechnics in Nigeria to build a cyber smart team capable of addressing evolving cyber threats and safeguarding national security. It highlights the current cybersecurity landscape in Nigeria, emphasizing the rising cyber risks and their potential impact on critical infrastructure and businesses. The author further discusses the role of polytechnics in bridging the cybersecurity skills gap by offering relevant programs and courses to equip students with essential cybersecurity knowledge and practical skills. Additionally, it emphasizes the importance of collaboration between polytechnics, industry stakeholders, and government agencies to develop comprehensive cybersecurity curricula, foster research and development, and promote industry-driven training initiatives that will ensure a secure digital future.

Keywords: cybersecurity, cyber smart team, polytechnic education, Nigeria

Published *31/05/2023*
Augustine N. Egere (2023). Building a Cyber Smart Team: The Imperative for Polytechnics in Nigeria. *Scholarly Journal of Science and Technology Research & Development*, 2(5), 13-19.

1.0. Introduction

The importance of cybersecurity cannot be overemphasized in today's rapidly evolving digital landscape. With the increasing number of cyber threats and attacks, organizations all over the world are realizing the importance of having a strong cybersecurity framework in place to protect their sensitive data and infrastructure. Nigeria, as a developing digital economy, is not immune to these challenges. To effectively counter cyber threats and safeguard the nation's digital assets, polytechnics in Nigeria must build cyber-smart teams equipped with the necessary knowledge and skills to address the evolving cyber landscape. According to the Global Cybersecurity Index (GCI) published by the International Telecommunication Union (ITU) in 2020, Nigeria ranked 37th out of 194 countries in terms of cybersecurity readiness. This ranking indicates that while the country has made some progress in cybersecurity, there is still significant room for improvement. Polytechnics, as institutions that offer technical education and training, have a unique opportunity to play a crucial role in enhancing Nigeria's cybersecurity preparedness. A study conducted by Oyewole and Adeoye (2021) emphasizes the importance of incorporating cybersecurity education and training into the curriculum of polytechnic institutions. The authors argue that by providing students with a solid foundation in cybersecurity principles, polytechnics can produce graduates who are equipped to tackle the complex challenges posed by cyber threats. Furthermore, the study highlights the need for hands-on training and practical experience to develop the skills required for cybersecurity professionals. To support the development of a cyber-smart workforce, collaboration between polytechnics and industry is essential. The Cybersecurity Maturity Model Certification (CMMC), a framework developed by the U.S. Department of Defense, emphasizes the importance of partnerships between academia and industry to cultivate cybersecurity talent. By establishing relationships with industry stakeholders, polytechnics in Nigeria can gain valuable insights into the latest cybersecurity trends and technologies, ensuring that their curriculum remains relevant and up-to-date. Additionally, initiatives such as the National Information Technology Development Agency (NITDA) National Cybersecurity Skills Development Program provide further impetus for polytechnics to prioritize cybersecurity education. The program aims to bridge the cybersecurity skills gap in Nigeria by offering training and certification programs for students and professionals alike. By actively participating in such initiatives, polytechnics can contribute to the national goal of building a skilled cybersecurity workforce. The recent unbundling of computer science as a course into cybersecurity, Artificial intelligence (AI), Networking, and web development is also a step in the right direction toward closing the skill gap (Nbte, 2023). It becomes very imperative for a cyber smart team to domicile at various polytechnics for easy collaborations among them and with the industry. Building a cyber-smart team is of utmost importance for polytechnics in Nigeria. By integrating cybersecurity education into their curriculum, fostering industry collaborations, and actively engaging in national initiatives, polytechnics can play a pivotal role in equipping the nation with a capable cybersecurity workforce. It is only through such concerted efforts that Nigeria can effectively combat cyber threats and safeguard its digital infrastructure.

2.0 The Cybersecurity Landscape in Nigerian Higher Education

Cybersecurity has become a critical issue for higher education institutions worldwide. Nigerian higher education institutions are no exception, facing various cybersecurity challenges such as data breaches, ransomware attacks, and phishing scams. A study by Ajiboye and Adewole (2021) reveals that Nigerian higher education institutions are vulnerable to cyber threats due to a lack of effective cybersecurity policies and strategies. The authors note that most institutions do not have a dedicated cybersecurity department or

personnel, and those that do, lack adequate resources to address cybersecurity challenges. The study further highlights the absence of regular security awareness training and education for students and staff, which leaves them susceptible to phishing scams and social engineering attacks. Another study by Akindele and Adeyemo (2020) reveals that Nigerian higher education institutions are also faced with the challenge of inadequate cybersecurity infrastructure. The authors argue that institutions need to invest in cybersecurity technologies such as firewalls, intrusion detection systems, and antivirus software to protect their digital assets. Additionally, the study notes the need for the establishment of Computer Emergency Response Teams (CERTs) in Nigerian higher education institutions to respond effectively to cyber threats.

The challenges faced by Nigerian higher education institutions in addressing cybersecurity threats are multifaceted. A study by Suleiman and Mohammed (2020) highlights the lack of regulatory frameworks and policies to guide cybersecurity practices in Nigerian higher education institutions. The study argues that the absence of such frameworks leaves institutions vulnerable to cyber threats and makes it challenging to hold them accountable for cybersecurity breaches. Additionally, the study notes the issue of insufficient funding as a significant challenge in addressing cybersecurity in Nigerian higher education. The authors contend that without adequate funding, institutions cannot invest in the necessary cybersecurity infrastructure and personnel to address cybersecurity threats effectively.

The cybersecurity landscape in Nigerian higher education, especially the polytechnics, is fraught with challenges that require urgent attention. Addressing these challenges requires a concerted effort by institutions, policymakers, and other stakeholders to establish robust cybersecurity policies and strategies, invest in cybersecurity infrastructure and personnel, and provide regular cybersecurity awareness training for staff and students. With these measures in place, Nigerian higher education institutions can mitigate the risks of cyber threats and safeguard their digital assets.

3.0 The Role and Benefits of a Cyber Smart Team

A cyber-smart team comprises skilled professionals responsible for implementing, managing, and enhancing the cybersecurity framework within an institution. This section delves into the key roles and responsibilities of a cyber-smart team, including incident response, threat intelligence, vulnerability assessment, awareness training, policy development, and security audits. The potential benefits of having a dedicated team, such as improved incident detection and response, enhanced risk mitigation, increased cybersecurity awareness, and strengthen regulatory compliance, are of great importance to the polytechnics in Nigeria.

Organizations face an increasing number of cybersecurity threats in today's interconnected world. Polytechnics have long been a source of semi-skilled and skilled labour in Nigeria, and they have much to offer in terms of keeping the country safe. To effectively combat these threats, polytechnics must establish a cyber smart team. This team is in charge of putting preventative measures in place, responding to incidents, and ensuring the overall security of digital assets. A cyber smart team's role and benefits in the context of cybersecurity include the following.

a. *Proactive Security Measures***:** A cyber smart team plays a pivotal role in implementing proactive security measures to prevent cyber threats. They conduct risk assessments, develop security policies, and implement controls such as firewalls, intrusion detection systems, and encryption protocols (Abu-Salma, 2021). By staying ahead of potential

threats, the team reduces the organization's vulnerability and strengthens its cybersecurity posture.

b. *Incident Response and Management:* When a cyber attack occurs, a cyber smart team is responsible for detecting, containing, and mitigating the impact of the incident (Choo, 2019). They promptly investigate the attack, identify compromised systems, and restore normal operations. Their expertise enables them to minimize damage, limit data loss, and preserve the organization's reputation.

c. *Security Awareness and Training:* Educating employees about cybersecurity best practices is essential to creating a culture of security within an organization. A cyber-smart team conducts security awareness campaigns and provides regular training to employees on topics such as password hygiene, phishing awareness, and safe browsing habits. This proactive approach reduces the likelihood of successful attacks that exploit human vulnerabilities.

Benefits of a Cyber Smart Team:

a. *Enhanced Security Posture*: By having a dedicated cyber smart team, polytechnics will significantly improve their security posture. These teams possess specialized knowledge and skills to identify, prevent, and respond to cyber threats effectively (Florencio et al., 2018). Their expertise helps in implementing robust security controls, reducing vulnerabilities, and mitigating risks.

b. *Timely Incident Response:* The presence of a cyber smart team ensures swift incident response and management. Their ability to detect and respond to cyber attacks promptly minimizes potential damage, reduces downtime, and accelerates the recovery process (Botta et al., 2019). This proactive approach mitigates financial losses and operational disruptions associated with cybersecurity incidents.

c. *Cost Savings*: While establishing a cyber smart team requires investment, it often leads to long-term cost savings. A study by the Ponemon Institute (2017) found that organizations with an incident response team experienced an average cost savings of $1.23 million per data breach incident. The team's capabilities to handle incidents efficiently and prevent future breaches contribute to these cost savings.

d. *Compliance and Regulatory Adherence:* In many industries, compliance with cybersecurity regulations is mandatory. A cyber smart team ensures that polytechnics meet the necessary regulatory requirements (Mishra et al., 2022). By staying up to date with the evolving landscape of cybersecurity regulations, the team helps the organization avoid legal penalties and reputational damage. A cyber smart team plays a critical role in protecting organizations from cyber threats. By implementing proactive security measures, managing incidents effectively, and fostering a culture of security awareness, these teams enhance an organization's security posture, reduce risks, and save costs (Wang et al., 2020). Their expertise and specialized knowledge contribute to the overall resilience and success of Polytechnics in the face of an ever-evolving cybersecurity landscape.

4.0 Implementing and Sustaining a Cyber Smart Team

Implementing and sustaining a cyber smart team is crucial for polytechnics aiming to enhance their cybersecurity posture and effectively mitigate cyber threats. This requires key steps and considerations.

i. *Assess Organizational Needs:* Before forming a cyber smart team, organizations like the polytechnic must assess their specific cybersecurity needs. This involves evaluating existing security measures, identifying vulnerabilities, and understanding the organization's risk appetite (Gondal et al., 2019). This assessment helps tailor the team's structure and responsibilities to address the organization's unique cybersecurity challenges.

ii. *Define Roles and Responsibilities*: Clearly defining the roles and responsibilities of team members is essential for a cyber smart team's effectiveness. Each team member should have well-defined responsibilities aligned with their expertise and the polytechnic's requirements (Yang et al., 2019). This clarity ensures efficient collaboration, accountability, and a comprehensive approach to cybersecurity.

iii. *Recruit and train team members:* Recruiting skilled professionals and providing ongoing training is critical for a cyber smart team's success. Qualified candidates should possess technical expertise in areas such as network security, incident response, and secure coding practices (Sengupta et al., 2020). Regular training and professional development programs keep team members updated on emerging threats, tools, and best practices.

iv. *Establish collaborative processes*: collaboration with other departments and stakeholders is vital for a cyber smart team's effectiveness. The team should establish processes for sharing information, coordinating incident response efforts, and ensuring cross-functional collaboration (Kshetri, 2017). These collaborative processes foster a culture of cybersecurity throughout the organization.

v. *Implement Technological Tools*: Equipping the cyber smart team with suitable technological tools enhances their capabilities. Tools such as security information and event management (SIEM) systems, vulnerability scanners, and threat intelligence platforms help in threat detection, incident response, and proactive security measures (Naik, *et al.*, 2022). The selection and implementation of tools should align with the organization's needs and budget.

vi. *Monitor and Evaluate Performance:* Regularly monitoring and evaluating the cyber-smart team's performance is crucial for continuous improvement. Metrics such as incident response time, the effectiveness of security controls, and staff training progress should be tracked (Dhillon et al., 2020). This data-driven approach helps identify areas for improvement and ensures the team's ongoing effectiveness.

Implementing and sustaining a cyber-smart team requires a well-planned approach, that considers organizational needs, defines roles and responsibilities, recruits skilled professionals, establishes collaborative processes, implements suitable technological tools, and monitors performance. By following these steps, the polytechnic can enhance its cybersecurity posture and effectively address the evolving cyber threat landscape.

Conclusion

Building a cyber-smart team is imperative for polytechnics in Nigeria to effectively address the growing cybersecurity challenges in the digital era. The establishment of a dedicated team equipped with the necessary skills and resources will help these institutions protect their digital assets, mitigate cyber threats, and foster a culture of cybersecurity awareness among

students and staff. By implementing proactive security measures, such as risk assessments and the deployment of cybersecurity technologies, polytechnics can significantly enhance their security posture. A cyber smart team will play a crucial role in incident response and management, promptly detecting and mitigating cyber attacks to minimize damage and downtime.

Furthermore, the team's responsibility for security awareness and training will empower students and staff with the knowledge and skills to identify and prevent cybersecurity threats. By fostering a cyber-smart culture, polytechnics can create a safer digital environment and reduce the risk of successful attacks. The challenges faced by polytechnics in Nigeria, such as the lack of cybersecurity policies and inadequate infrastructure, highlight the urgent need for a dedicated cyber smart team. These teams can work towards establishing robust cybersecurity frameworks, leveraging resources effectively, and advocating for necessary investments in cybersecurity infrastructure.

In conclusion, polytechnics in Nigeria must recognize the imperative of building a cyber-smart team to address the ever-evolving cybersecurity landscape. By investing in skilled personnel, advanced technologies, and comprehensive training programs, these institutions can enhance their resilience against cyber threats, protect sensitive data, and provide a secure learning and working environment for their stakeholders. The establishment of a cyber smart team is a critical step towards safeguarding the digital future of Nigerian polytechnics.

References

Abu-Salma, R. (2021). Cybersecurity and cyberdefense In Cyber Security Engineering (pp. 115-132). Springer.

Ajiboye, O. B., & Adewole, K. S. (2021). Cybersecurity challenges in Nigeria's higher education: A qualitative study. International Journal of Education and Development using information and communication technology, 17(1), 52–68.

Akindele, A. A., & Adeyemo, S. A. (2020). Cybersecurity Challenges in Nigeria universities: A review. Journal of Information Security, 11(3), 204–217

Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2019). Integration of cloud computing and the Internet of Things: A Survey of Future Generation.

Choo, K.-K. R. (2019). Incident response and management. In K.-K. R. Choo (Ed.), Cybercrime: The investigation, prosecution, and defense of a computer-related crime (3rd ed., pp. 287–310).

Dhillon, G., Backhouse, J., & Hsu, C. (2020). Cybersecurity: Managing systems, conducting testing, and investigating intrusions. CRC Press.

Gondal, I. A., Ahmad, R., & Hussain, Z. (2019). Cybersecurity capability assessment: A systematic literature review. Journal of Systems and Software, 151, 100–114.

Florencio, D., Herley, C., & Van Oorschot, P. C. (2018). Passwords and cyber security: A review. Journal of Economic Surveys, 32(3), 828-854

International Telecommunication Union (ITU). (2020). Global Cybersecurity Index 2020. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2020.aspx

Kshetri, N. (2017). Big data's roles in improving cyber security: A longitudinal study of IT security professionals. Information Systems Frontiers, 19(3), 449–466.

Mishra A, Alzoubi YI, Gill AQ, Anwar MJ.(2022) Cybersecurity Enterprises Policies: A Comparative Study. Sensors (Basel). 22(2)

Naik, B., Mehta, A., and Yagnik, H. (2022). The impacts of artificial intelligence techniques in Augmentation of cybersecurity: a comprehensive review. *Complex Intell. Syst.* **8**, 1763–1780.

National Board for Technical Education (2023), Unbundling Computer Science programmes in Polytechnics, Retrieved from https://www.Nbte.gov.ng

Ponemon Institute. (2018). 2018 Cost of Data Breach Study: Global Overview. Retrieved from https://www.ibm.com/security/data-breach

Oyewole, O., & Adeoye, S. (2021). The integration of cybersecurity into tertiary education: Evidence from polytechnics in Nigeria. Journal of Computer Sciences and Applications, 9(1), 9-16.

Sengupta, S., Ray, P. K., & Rao, H. R. (2020). Developing a cybersecurity workforce: Exploring current practices and proposing a curriculum. Journal of Information Systems Education, 31(3), 151-162.

Suleiman, I., & Mohammed, I. (2020). Cybersecurity challenges in Nigerian higher education: A critical analysis. International Journal of Emerging Technologies in Learning, 15(12), 201-217.

Yang, L., Yue, H., Chen, J., Wang, Y., & Liang, X. (2019). A flexible resource allocation method for the cybersecurity capability of complex systems. Computers & Electrical Engineering, 78, 272-287.

Wang, Y., Tong, Y., Liu, H., Li, Z., & Yang, L. T. (2020). Cybersecurity framework for Internet of things: A systematic review. ACM Computing Surveys, 53(4), 1-37.