International Journal of Applied Mathematics, Sciences, and Technology for National Defense
Volume 3, Issue 3, 131-142
e_ISSN: 2985-9352, p_ISSN: 2986-0776
https://www.journal.foundae.com/index.php/JAS-ND
DOI : https://doi.org/10.58524/app.sci.def.v3i3.780

Towards a standard framework for cybersecurity readiness for Nigerian universities

Olusegun Hamed Olugbile*
Nasarawa State University Keffi
NIGERIA

J. A. Ojeniyi
Nasarawa State University Keffi
NIGERIA

Tochukwu Kene Anyachebelu
Nasarawa State University Keffi
NIGERIA

Article Info

Article history:

Received: June 11, 2025
Revised: October 15, 2025
Accepted: October 30, 2025
Published: December 30, 2025

Keywords:

Cybersecurity Readiness Index
Cybersecurity Readiness Tiers Framework
Principal Component Analysis
Risk Assessments
Universities

Abstract

Universities rely substantially on digital infrastructure and host vast amounts of data that are of interest to malicious actors. Thus, they are vulnerable to cyber-attacks, making their protection a significant issue. While technology continues to improve, educational system infrastructures and system security lag behind. However, to ensure the continuous availability of university digital assets, the infrastructure must be prepared to withstand cyber-attacks. The results of research indicate that several models exist for evaluating the readiness of universities for cybersecurity. These models have been established for developed nations with more sophisticated and mature cyber networks and may not be directly applicable to developing economies like Nigeria. Therefore, the Design Science Research strategy was adapted to develop a framework for assessing cybersecurity readiness in Nigerian universities. Taking into account pre-event, event management, and post-event factors, the concept of Cybersecurity Readiness Tiers (CRT) was developed to compare the cybersecurity readiness of universities. The Cybersecurity Readiness Framework was evaluated using data collected from candidate universities sampled for this study; Principal Component Analysis was carried out on the dataset to reduce the dimension. The Cybersecurity Readiness Index (CRI) scores, along with their respective distributions, indicate that 14 (65%) of the twenty universities fall in T1, while 6 (35%) fall in T2. The grouping was based on their overall cybersecurity readiness, as computed using the mathematical equations of the framework. Thus, it implies universities in T2 have a high level of readiness to resist cybersecurity incidents, while universities in T1 are at a very low level of readiness due to the weak and inconsistent cybersecurity controls implemented. This study suggests that these universities have gaps in event management and post-event capabilities that require attention. Therefore, a holistic web-based Cybersecurity Assessment tool that will incorporate all security and privacy regulations and best practices can be considered for future studies.

To cite this article: Olugbile, H. O., Ojeniyi, J. A., & Anyachebelut, T. K. (2025). Towards A Standard Framework for Cybersecurity Readiness for Nigerian Universities. *International Journal of Applied Mathematics, Sciences, and Technology for National Defense,* 3(3), 131-142

INTRODUCTION

Background

Cyberspace rapidly became a global phenomenon in the twenty-first century, where personal, professional, and corporate lives are increasingly intertwined (Garba & Bade, 2021). Cyberspace refers to the electronic world created by interconnected networks of information technology and the information on those networks; sometimes, the term "cyber" is not only used to refer to technology but also a political idea that is embedded in numerous technologies (Badamasi & Utulu, 2021).

***Corresponding Author:**
Olusegun Hamed Olugbile, Nasarawa State University Keffi, Nigeria, Email: olugbileolusegun00006@nsuk.edu.ng

However, in the education sector, teachers and students make use of the ever-expanding resources available over the internet by creating a diverse learning experience that caters to many teaching and learning styles. Any information sent via the internet carries the risk of being compromised without the sender's knowledge, due to the ongoing development of cybersecurity as the computer age progresses (Demirkan et al, 2020; Kulugh et al., 2022).

Due to the ongoing digital revolutions, universities are increasingly becoming targets of malicious cyber activities. This vulnerability arises from the vast amounts of information and accumulated knowledge they possess, making them attractive to threat actors. These attackers often seek to exploit research findings, financial data, and computing resources. According to Aliyu et al. (2020), universities are among the riskiest environments for individuals to disclose sensitive information. The claim is in conformity with recent cybercrime incidents that occur in Nigerian universities (Badamasi & Utulu, 2021) reaffirming that universities in Nigeria are not well-prepared to defend against or recover from cyber-attacks. However, to effectively manage cybersecurity incidents, it is essential to plan for cybersecurity risks, which involves implementing adequate measures to prevent cyberattacks and mitigate their effects if they occur (Eaton et al., 2019). Cybersecurity is an essential component of a network infrastructure's efficient operation, which has been integrated with information and communications technology (Makridis & Smeets, 2018).

Consequently, a significant security risk and vulnerability are considered to have restricted the growth and acceptability of the digital revolution in Nigerian universities. Therefore, how the transitions towards a digital system will affect the cybersecurity of an institution should be considered prior to the adoption of any new technology. Although determining the level of cybersecurity preparation, resilience, and contingency is the goal of cyber-attack readiness (Alsmadi et al., 2022). Cybersecurity readiness refers to the ability to identify, detect, prevent, and respond effectively to cyber threats and incidents. It measures how well-maintained vital institution infrastructure and operations can be in the event of a cyber-attack. Bahuguna et al. (2020) notes that security assessments provide institutions with a comprehensive understanding of the attitudes, behaviors, and potential threats that may impact their cyber assets. To examine the current state of cybersecurity readiness in Nigerian universities, this study developed a cybersecurity readiness framework by analyzing pre-attack activities, event management, and post-attack activities to iteratively assess the information and communication technology (ICT) infrastructure and operational best practices within the university system (Nehrey et al., 2022; Rupra & Omamo, 2020).

Developing nations face numerous challenges in protecting their physical hardware, software infrastructure, and internet-hosted data from cyber-attacks. While computers and the internet are essential tools for students' and teachers' daily interactions, they are also preferred targets that attackers increasingly use against them. The cybersecurity risks associated with digital assets in Nigerian universities have been significantly impacted by factors such as data security, data privacy, and a lack of cybersecurity awareness (Georgiadou et al., 2022a; Georgiadou et al., 2022b). Many organisations have attempted to protect their information using technological approaches, such as Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and Security Information and Event Management (SIEM). Consequently, security breaches occur as a result of the new development of either hardware or software. This new device results in new vulnerabilities (Hasan et al., 2021; Sharma & Venkatraman, 2023).

In terms of Nigeria's institutional cybersecurity challenges, the top 5 areas for 2016 were: awareness and training, ongoing monitoring and log analysis, vulnerability management and patching, ongoing risk assessment and management, managed service, and independent review (Beuran et al., 2023; Khan et al., 2021). Therefore, there is a need for universities to have in place a framework that measures their cybersecurity posture to continuously protect their assets as technology and information security evolves, and a thorough examination of cybersecurity readiness is essential in order to swiftly and effectively launch a successful digital transition plan (Kusmiarto et al., 2021). However, research on cybersecurity readiness and solutions in universities is particularly minimal. Thus, this study proposes addressing this gap by having a tool that universities can use to measure their cybersecurity readiness and compliance levels to adopt new technology with minimal cybersecurity risk. Based on this background, several issues have arisen, including:

a) What are the cybersecurity metrics that can be used to evaluate the cybersecurity readiness of Nigerian universities?

b) How can an appropriate cybersecurity readiness framework be developed for Nigerian Universities?
c) How can the framework for cybersecurity readiness be validated?

NIST Cybersecurity Framework

In an era marked by rapid technological progress and an ever-expanding digital landscape, businesses face an unprecedented level of cyber threats. To counter these evolving and complex attacks, a robust cybersecurity resilience framework has become essential (Too et al., 2022). Today's businesses operate within an increasingly interconnected landscape, making them vulnerable to various cyber threats that can compromise data integrity, disrupt operations, and damage their reputation. Thus, establishing a comprehensive cybersecurity resilience framework is crucial for fortifying defenses and ensuring business continuity (Foomin et al., 2008; Ilori et al., 2024).

To examine ways to enhance security and ensure that the organization's sensitive data, assets, and other resources are properly protected. The framework's five concurrent and continuous core functions—Identify, Protect, Detect, Respond, and Recover — are a risk-based method for managing cybersecurity risk (NISTCSF 2.0) as illustrated in figure 1. These functions provide a comprehensive and strategic view of an organization's lifecycle management of cybersecurity risks when considered collectively and embedded with a governance framework (NIST, 2018). Functions simultaneously support govern, identify, protect, and detect, while enabling respond and recover during cybersecurity incidents. Govern, identify, and protect, focusing on prevention and preparation, while govern, detect, respond, and recovering, aids in incident identification and management.

Figure 1. NIST Cybersecurity framework (NIST, 2024).

ISO/IEC27001 Standard

Two international organizations that set best practice standards for various industries globally are the International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO). According to Culot, et al. (2021), the JTCs of ISO and IEC collaborate in areas of shared interest. All organisations, regardless of their form, size, or nature, are expected to comply with the requirements outlined in ISO/IEC 27001:2013. According to Obotivere and Nwaezeigwe (2020), threats can be derived from two primary sources: human activities and natural events.

i. Human threats are those brought about by individuals, such as malicious threats that are either internal or external, which aim to harm or disrupt a system.
ii. Natural threats, such as earthquakes, hurricanes, floods, and fire, could cause severe damage to computers.
iii. Systems and nobody can

Deterrence Theory

Information systems researchers have utilized deterrence theory to examine compliance with information security policy since it was first developed by criminology scholars (Soomro & Hussain,

2019). According to Jacobs (2010), deterrence theory can be used to better comprehend the laws and guidelines issued by national and international bodies to control and regulate business activities. Wall et al. (2016), discusses organizational rule enforcement and sanctions using the deterrence theory.

According to Obotivere & Nwaezeigwe (2020), vulnerability is a cybersecurity term that refers to a fault or weakness inherent in a system that exposes information security to threats or attacks. There are two types of vulnerabilities: hardware and software.

The Global Cybersecurity Index (GCI)

The Global Cybersecurity Index (GCI) is a reputable tool developed by the ITU that assesses a nation's commitment to cybersecurity on a global scale, highlighting the significance and various facets of the problem. Each nation's level of growth or engagement is evaluated along five pillars due to the wide range of applications for cybersecurity that cut across numerous businesses and sectors:

a) Legal Measures
b) Technical Measures
c) Organizational Measures
d) Capacity Development, and
e) Cooperation

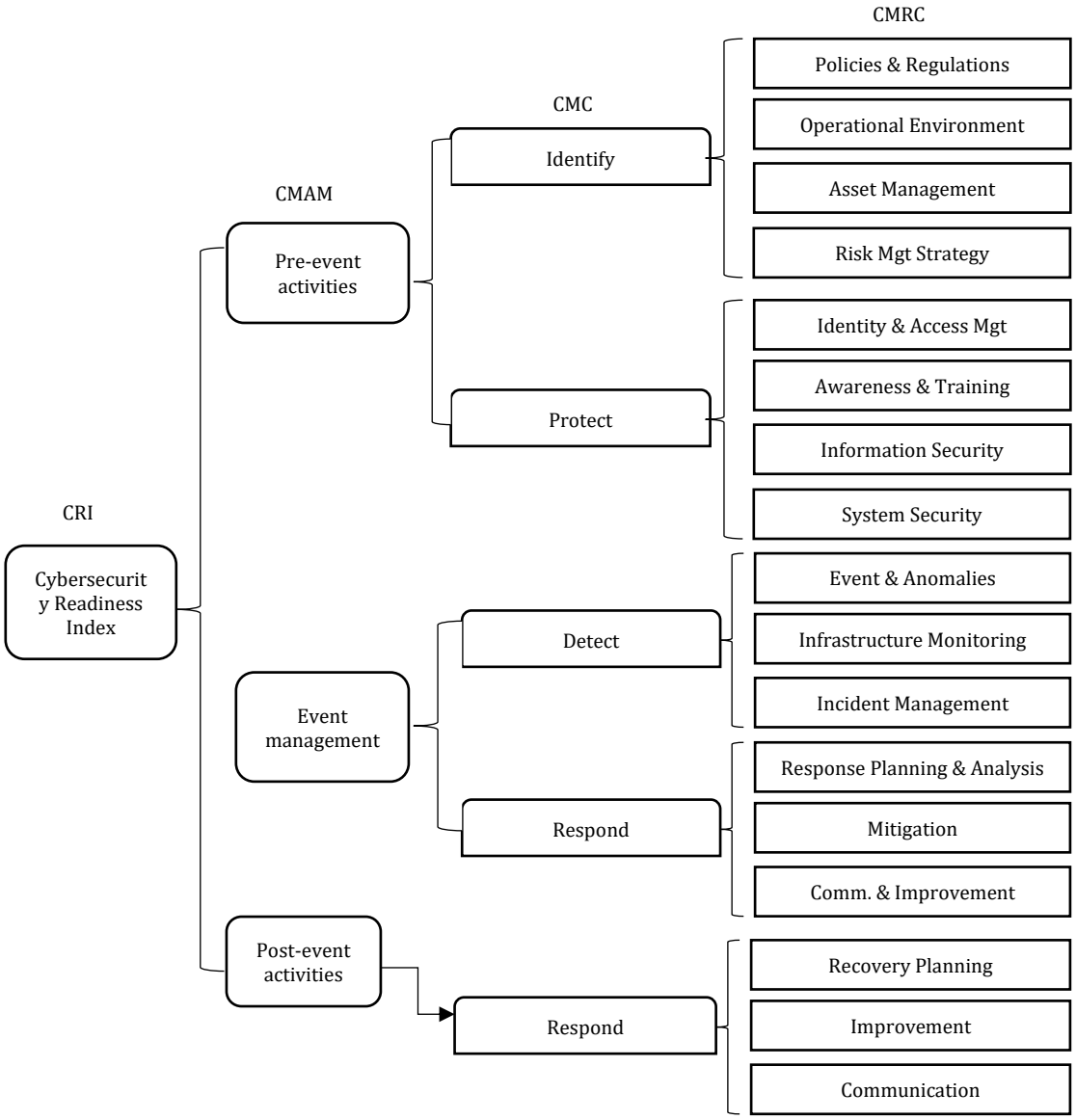

Figure 2. Cybersecurity Readiness Framework

METHOD

Cybersecurity Maturity Measures (CMM)

Measurable cybersecurity requirements are defined by the Cybersecurity Maturity Measures (CMM) for the purpose of quantifying readiness (Sharkov, 2020). The CMM provides baseline metrics and indicators upon which cybersecurity readiness can be measured as shown in figure 2. Similar to the CMRC, the CMM draws its components from NIST' framework, and ISO/IEC27001 Standards. The CMMs are measured based on the scale of Cybersecurity Maturity Measures (CMM) defined in Table 1.

Its quantitative weights offer equal spacing between adjacent levels of the CMM and are defined on a 4-level ratio scale between 0 and 3. This is appropriate given that the ratio scale progresses from zero to larger weights. Zero denotes the absence of control, which is essential for quantitative measurement, as noted by Uher (2018). The CMM is described in great details in Table 1

Table 1. Cybersecurity Maturity Measure Scale (Uher ,2018).

Weight	Qualitative	Descriptions
0	Not accomplished	Cybersecurity controls are completely absent.
1	Loosely accomplished	Cybersecurity controls are weak and inconsistently implemented
2	Partially accomplished	Moderate cybersecurity controls are in place, but they are not consistently and properly organized, and many or all of the necessary components are absent.
3	Largely accomplished	Cybersecurity controls are structurally implemented, but some components of are missing.

Cybersecurity Maturity Requirement Category (CMRC)

The CMRC elements are the requirements categories of the Cybersecurity Maturity Controls (CMC); identify, protect, detect, respond, and recover as part of CRF structures with their sub-categories CMMs, as shown in Figures 2, 3, 4, 5, and 6 respectively.

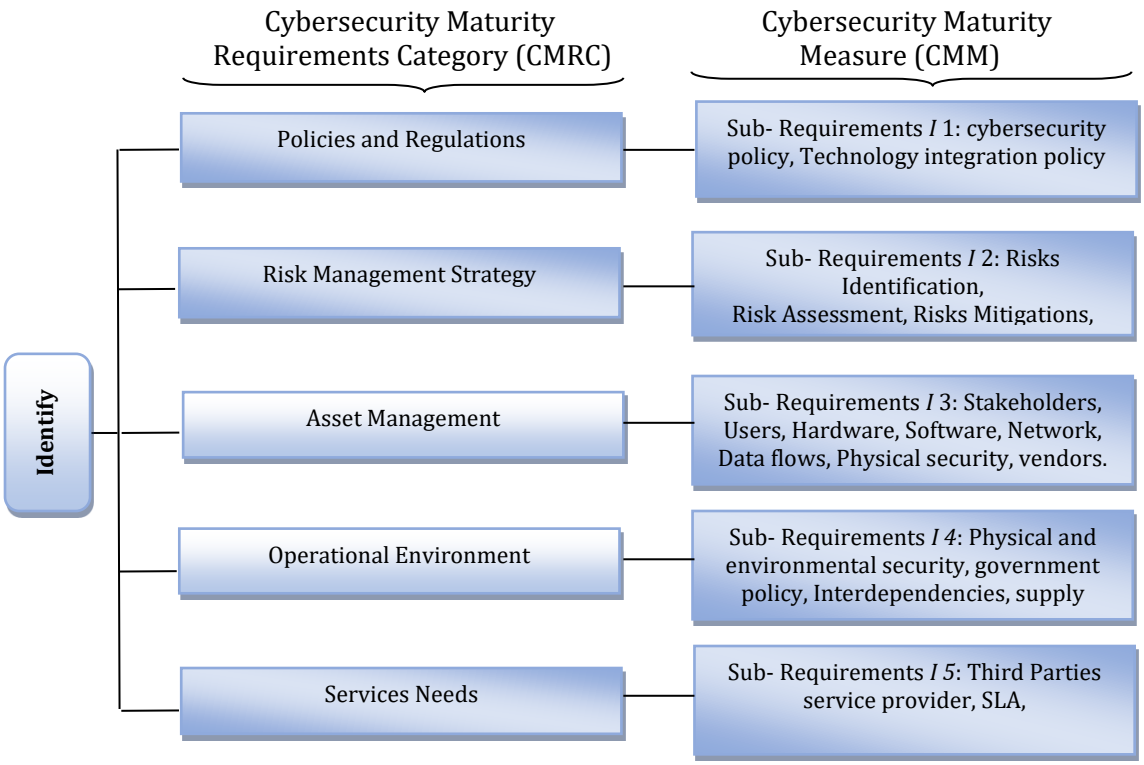

Figure 3 .Cybersecurity Maturity Control; Identify.

The identify of CMC in the framework core is detailed in Figure 3. The CMRCs and CMMs of the CMC's identity are contained inside. The CMM gives information on what is to be measured per CMRC elements, while the CMRC provides details on the elements that measure the policies and regulations, asset management, and operational environment. For instance, assets management can be assessed based on the identification of hardware, software, network map, physical security, data flow, user, etc.

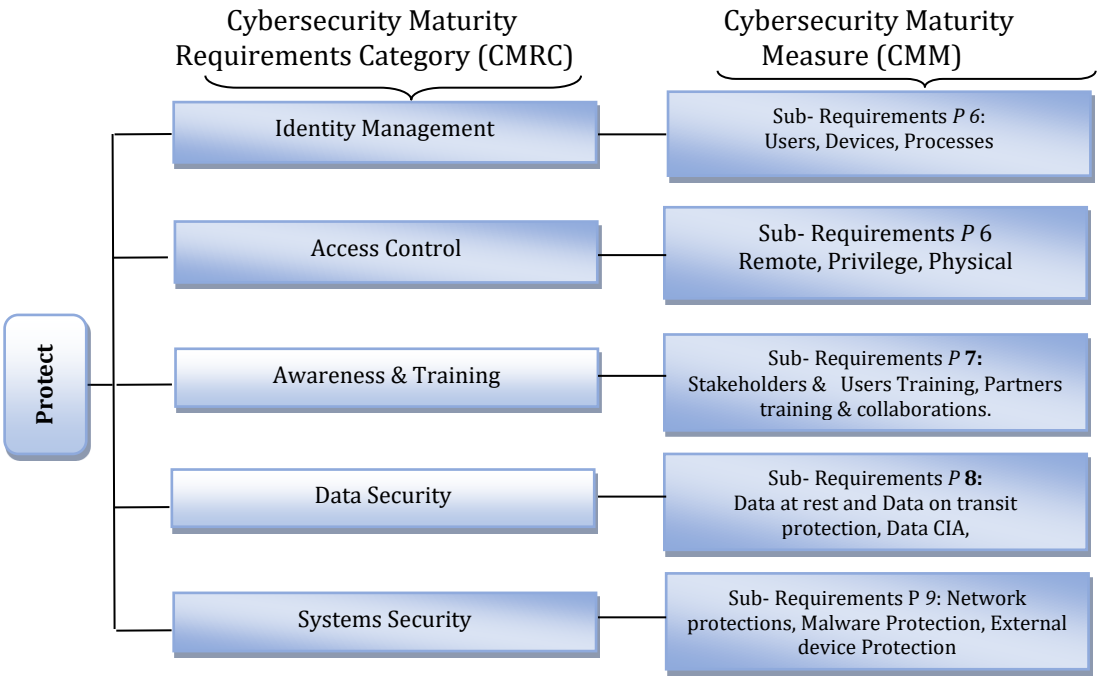

Figure 4. Cybersecurity Maturity Control; Protect.

The protect CMC in the CRF core is described in full Figure. 4. It includes the CMRC and CMM of the protect CMC. The CMRC outlines the components that evaluate an institution's protection capacity, while the CMM defines the specifics of the component that will be evaluated. The degree of network availability, malware protection, and other factors, for instance, can be used to quantify protective control.

Table 2 below shows the mapping of CMCs into the CMAMs. For instance, the Identify (I) & Protect (P), CMCs are mapped to pre-event activities CMAMs, the Detect (D) & Respond (R) CMCs are mapped to event management CMAMs, and the Recover (R) CMCs are mapped to post-event activities CMAMs, respectively.

Table 2. Mapping of CMCs to CMAMs

	Cybersecurity Maturity Assessment Metrics (CMAM)	cybersecurity Maturity Assessment Controls (CMC)
1	Pre-Event Act	Identify Protect
2	Event Management	Detect Respond
3	Post-Event Act	Recover

Table 3 provides information on the three cybersecurity maturity assessment metrics that are shown in the framework in figure 4.1, as well as their descriptions and weightings when determining an institution's level of cybersecurity readiness. The impact of each event could vary greatly, therefore it is unlikely that the contributing elements to these high-level measurements will be equal. To reflect individual contributions, the event effects can be expressed as weights.

Table 3. Cybersecurity Maturity Assessment Metrics Weights

Weight	Qualitative	Descriptions
0	Not accomplished	Cybersecurity controls are completely absent.
1	Loosely accomplished	Cybersecurity controls are weak and inconsistently implemented
2	Partially accomplished	Moderate cybersecurity controls are in place, but they are not consistently and properly organized, and many or all of the necessary components are absent.
3	Largely accomplished	Cybersecurity controls are structurally implemented, but some components of are missing.

The tiers are labeled as T1 and T2, based on CRI scores of individual universities. Each value in the range defines the maturity level of a candidate university. The research is defined in Table 4. The table also provides a detailed interpretation of each tier.

Table 4. Cybersecurity Maturity Tiers (CMT)

Tiers	**Range**	**Interpretations**
T1	0.0 – 0.49	The institution is at a very low level of maturity for cybersecurity incidences due to the weak and inconsistently cybersecurity controls implemented.
T2	0.50 – 1.00	Best practices in cybersecurity are fully implemented. This implies that the level of cybersecurity readiness is very high.

Since the research on cybersecurity readiness index for university education system have not been founded at the time of the study, to address the research question (1), this study relies on previous literatures and theories such as Deterrence theory, ISO/IEC27001 Standard and NIST cybersecurity framework that have been used in similar discipline, as the basic of this research. The development of the survey items began with a review of the literature. The construct items of the framework were developed based on existing construct items in previous research, particularly the ISO/IEC27001 Standard and NIST cybersecurity framework, to ensure the greatest possible reliability and validity of the items. Additionally, several new constructs were developed based on the definitions of the framework constructs presented in this study. The appendix page presents all constructs, along with the number of measurement items used in the study. The respondents were asked to measure the construct items defined on a 4-level rating scale, ranging from 0 to 3 (0 = 'Not accomplished', 1 = 'Loosely accomplished', 2 = 'Partially accomplished', 3 = 'Largely accomplished'). The respondents were also asked to provide demographic data about themselves and their respective institutions.

The final survey was sent to approximately 20 selected IT professionals from different universities as sampled in the study. This respondent pool was selected as the most knowledgeable about information security in their individual institutions, since not all institutional staff are cybersecurity experts. The survey was sent as soft copies via Google Forms and distributed by sending invitations, which included a link to the Google form. A total of 18 responses were received, representing 80% response rate. The online questionnaires were checked, and a well-coded summary was provided. Principal Component Analysis (PCA) was carried out on the dataset in reducing the dimension.

RESULTS AND DISCUSSION

Result of the Data Analysis

Data was collected through a questionnaire method from the candidates' universities sampled for the research to test the effectiveness of the framework. Thus, Principal Component Analysis (PCA)-based dimensionality reduction was employed to reduce the dataset's dimension from 30 features to 10 principal components. The cumulative explained variance ratio plot indicated that the 10 principal components accounted for 95% of the variance in the data.

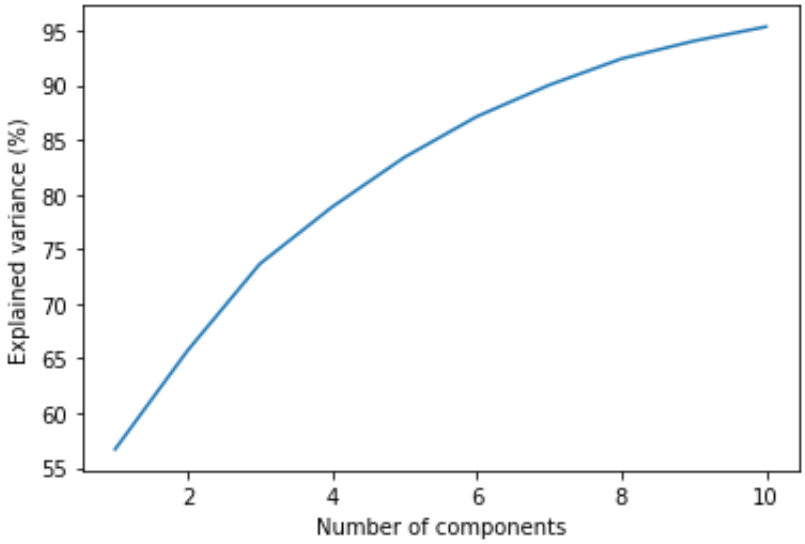

Figure 5. Percentage Variance for each Principal Component

Figure 5 shows the relationship between variance and number of components; the larger the variance carried by a line, the more information it has. Figure 5 represents the 20 universities' Cybersecurity Readiness Index (CRI) scores with their respective distribution in Cybersecurity Maturity Tiers (CMT) as defined in Table 4.

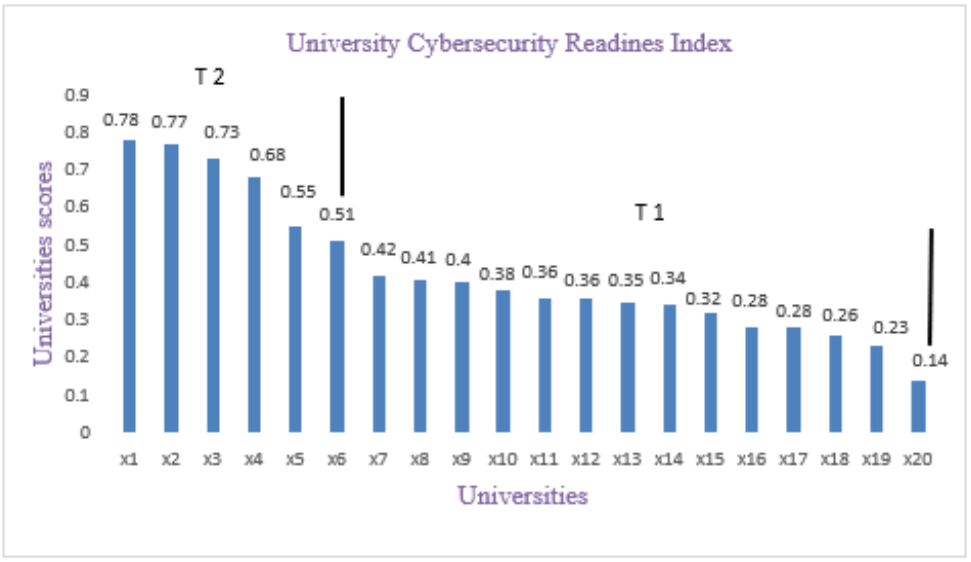

Figure 6 . Cybersecurity Readiness Index

The scores as indicated show that 14(65%) of the 20 universities fall in T1, with 6(35%) in T2, respectively. The grouping was based on their overall cybersecurity readiness, as computed using the mathematical equations of the framework. Thus, it implies that universities in T2 have a high level of readiness to resist cybersecurity incidents, whereas universities in T1 are at a very low level of readiness for cybersecurity incidents due to the weak and inconsistent cybersecurity controls implemented.

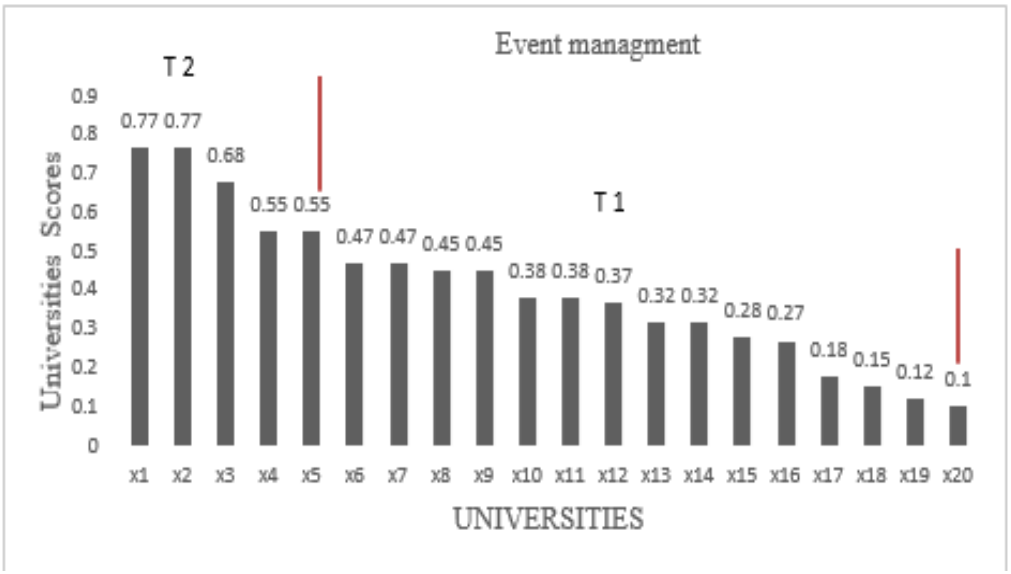

Figure 7. Event management

The survey shows that most universities have cybersecurity controls in place. However, these controls are not consistently and properly organized or managed, which reduces their effectiveness in mitigating the severity of cyber-attacks.

Discussion of Findings

The design of the cybersecurity readiness framework for the Nigerian university system was based on the identified security controls from the ISO/IEC 27001 Standard and the NIST Cybersecurity Framework, with a focus on how security controls, policies, strategies, governance, and stakeholders' characteristics influence technology usage within university systems.

The cybersecurity controls and the mathematical model for cybersecurity readiness comprise the two main components of the CRF. The computational constructs of the cybersecurity controls were developed using a mathematical model generated from the requirement categories, and these constructs serve as the foundation for the quantitative evaluation of a university's cybersecurity readiness level.

The assessments of cybersecurity readiness were conducted using the methodology at 20 universities. The names of the universities were replaced with 1-letter codes for anonymity. The assessment considered three (3) Cybersecurity Maturity Assessment Metrics, Pre-event activities, Event Management, and Post-event activities, as well as the five (5) Cybersecurity Maturity Controls were employed to evaluate the framework.

The scores, as indicated in Figure 7, show that 14(65%) of the twenty universities fall in T1, with 6(35%) in T2, respectively. It can be inferred from this analysis, based on Table 4.1, that 35% of the evaluated universities achieved a high level of readiness, indicating the implementation of cybersecurity controls and best practices, while 65% are in the managed and defined stage of low cybersecurity readiness.

The results also suggest that using PCA-based dimensionality reduction can be an effective approach for reducing the dimensionality of high-dimensional datasets without significantly compromising model performance.

CONCLUSION

There are many advantages to cybersecurity, but also a few drawbacks. Organisations that handle sensitive information and lack cybersecurity expertise, such as those in the educational sector, are at great danger from cyberattacks. It is beneficial to the organization's defence against cybercrimes to hire a role to carry out cybersecurity operations. Additionally, institutions have a responsibility to provide their staff with appropriate cybersecurity training. These assist staff members in early attack detection, which may not be effective in defending against the attack but may aid in limiting the loss. Even while this inadvertently teaches workers how to carry out insider attacks

covertly, this can be mitigated by implementing constant surveillance and security measures. The study identified further opportunities for improvement in university settings, such as inadequate security procedures to defend against and recover from potential cyberattacks.

Users need to be made more aware that everyone is responsible for cybersecurity, not just the ICT professionals, and that infrastructure plays a role in enhancing secure access. As a result, the vital infrastructure of higher education institutions should place a greater priority on cybersecurity. This is in line with the ITU's observations regarding the necessity of cybersecurity policies that take into account the significance of cyberspace safety; support private and public partnerships; build user awareness; empower human capital to identify cybersecurity problems; involve technical staff in the design of solutions; and share the responsibility for having a safe and resilient cyberspace with users.

A comprehensive web-based cybersecurity assessment tool that incorporates all security and privacy regulations and best practices should be considered in future studies.

AUTHOR CONTRIBUTIONS

O.H.O.: Conceptualization, formal analysis, methodology, & writing – original draft. J.A.O. and T.K.A.: Formal analysis, investigation, resources, and writing – review & editing.

CONFLICT OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. *Applied Sciences*, 10(10), 3660, 1-15. https://doi.org/10.3390/app10103660

Alsmadi, I., Tsado, L., & Gibson, C. (2022). Cyber readiness assessment in rural areas: A systematic literature review. *SSRN Electronic Journal*, 4311195, 1-4. https://doi.org/10.2139/ssrn.4311195

Badamasi, B., & Utulu, S. C. A. (2021). Framework for managing cybercrime risks in nigerian universities. *arXiv preprint arXiv:2108.09754*. https://doi.org/10.48550/arXiv.2108.09754

Beuran, R., Vykopal, J., Belajová, D., Čeleda, P., Tan, Y., & Shinoda, Y. (2023). Capability assessment methodology and comparative analysis of cybersecurity training platforms. *Computers & Security*, 128, 103120. https://doi.org/10.1016/j.cose.2023.103120

Bahuguna, A., Bisht, R. K., & Pande, J. (2020). Country-level cybersecurity posture assessment: study and analysis of practices. *Information Security Journal: A Global Perspective*, 29(5), 250-266. https://doi.org/10.1080/19393555.2020.1767239

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *The TQM Journal*, 33(7), 76-105. https://doi.org/10.1108/TQM-09-2020-0202

Makridis, C. A. & Smeets, M. (2019). Determinants of cyber readiness. *Journal of Cyber Policy*, 4(1), 72-89. https://doi.org/10.1080/23738871.2019.1604781

Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics*, 7(2), 189-208. https://doi.org/10.1080/23270012.2020.1731721

Eaton, T. V., Grenier, J. H., & Layman, D. (2019). Accounting and cybersecurity risk management. *Current Issues in Auditing*, 13(2), C1-C9. https://doi.org/10.2308/ciia-52419

Fomin, V. V., Vries, H., & Barlette, Y. (2008). ISO/IEC 27001 information systems security management standard: exploring the reasons for low adoption. *EuroMOT 2008 - The Third European Conference on Management of Technology*, 1-13.

Garba, A. A. & Bade, A. M. (2021). The current state of cybersecurity readiness in nigeria organizations. *International Journal of Multidisciplinary and Current Educational Research (IJMCER)*, 3(1), 154 -162. https://www.ijmcer.com/volume-3-issue-1/

Georgiadou, A., Michalitsi-Psarrou, A., & Askounis, D. (2022). Cyber-security culture assessment in academia: A covid-19 study: applying a cyber-security culture framework to assess the

academia's resilience and readiness. *In Proceedings of the 17th International Conference on Availability, Reliability and Security*, 126, 1-8. https://doi.org/10.1145/3538969.3544467

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A cyber-security culture framework for assessing organization readiness. *Journal of Computer Information Systems*, 62(3), 452-462. https://doi.org/10.1080/08874417.2020.1845583

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, 58, 102726. https://doi.org/10.1016/j.jisa.2020.102726

Ilori, O., Nwosu, N. T., & Naiho, H. N. N. (2024). A comprehensive review of it governance: effective implementation of COBIT and ITIL frameworks in financial institutions. *Computer Science & IT Research Journal,* 5(6), 1391-1407. https://doi.org/10.51594/csitrj.v5i6.1224

ISO Standards (2018) ' ISO 31000:2018 Risk management – Guidelines. International

Jacobs, B. A. (2010). Deterrence and deterrability. *Criminology,* 48(2), 417-441. https://doi.org/10.1111/j.1745-9125.2010.00191.x

Khan, S. K., Shiwakoti, N., Stasinopoulos, P., & Matthew, W. (2021). Dynamic assessment of regulation and policy framework in the cybersecurity of Connected and Autonomous Vehicles. *In Australasian Transport Research Forum, ATRF 2021-Proceedings*, 1-12.

Kulugh, V. E., Mbanaso, U. M., & Chukwudebe, G. (2022). Cybersecurity resilience maturity assessment model for critical national information infrastructure. *SN Computer Science*, 3(3). https://doi.org/10.1007/s42979-022-01108-x

Kusmiarto, K., Aditya, T., Djurdjani, D., & Subaryono, S. (2021). Digital transformation of land services in Indonesia: A readiness assessment. *Land*, 10(2), 1-16. https://doi.org/10.3390/land10020120

NIST. (2018). Framework for improving critical infrastructure cybersecurity. https://doi.org/10.6028/NIST.CSWP.04162018

Nehrey, M., Voronenko, I., Salem, A. B. M. (2022). Cybersecurity Assessment: World and Ukrainian Experience. *In 2022 12th International Conference on Advanced Computer Information Technologies (ACIT)*, 335-340. https://doi.org/10.1109/ACIT54803.2022.9913081

Obotivere, B. A. & Nwaezeigwe, A. O. (2020). Cyber security threats on the internet and possible solutions. *International Journal of Advanced Research in Computer and Communication Engineering,* 9(9), 92-97. https://doi.org/10.17148/IJARCCE.2020.9913

Rupra, S. S. & Omamo, A. (2020). A cloud computing security assessment framework for small and medium enterprises. *Journal of Information Security,* 11(4), 201-224. https://doi.org/10.4236/jis.2020.114014

Soomro, T. R., & Hussain, M. (2019). Social media-related cybercrimes and techniques for their prevention. *Applied Computer Systems*, 24(1), 9–17. https://doi.org/10.2478/acss-2019-0002

Sharma, A., & Venkatraman, S. (2023). Towards a standard framework for organizational readiness for technology adoption. *In Advances in Digital Manufacturing Systems: Technologies, Business Models, and Adoption* (pp. 197-219). Springer Nature Singapore. https://doi.org/10.1007/978-981-19-7071-9_10

Sharkov, G. (2020). Assessing the maturity of national cybersecurity and resilience. *Connections: The Quarterly Journal*, 19(4), 5-24. https://doi.org/10.11610/Connections.19.4.01

Too, W. K., Karume, S. M., & Masese, N. B. (2022). Defensive cybersecurity preparedness assessment model for universities. *International Journal of Computer (IJC)*, 43(1), 112-128. https://ijcjournal.org/InternationalJournalOfComputer/article/view/1950

Uher, J. (2018). Quantitative data from rating scales:an epistemological and methodological enquiry. *Frontiers in Psychology,* 9(2599), 2018. https://doi.org/10.3389/fpsyg.2018.02599

Wall, J., Lowry, P. B., & Barlow, J. B. (2016). Organizational violations of externally governed privacy and security rules: explaining and predicting selective violations under conditions of strain and excess. *Journal of the Association for Information Systems*, 17(1), 39-76. https://doi.org/10.17705/1jais.00420