Kontagora International Journal of Educational Research (KIJER) ISSN: 3027-0618
Volume 2, Issue 2, March 2025
https://fuekjournals.org/index.php/kijer

An Analysis of Cybersecurity Culture Among the Nigerian Academia

OYEFESO OLUFEMI OLANREWAJU

Corresponding author: *femolapel@gmail.com* 07067901231

Federal University of Education Kontagora, Niger State, Nigeria

To cite:
Oyefeso, O. O. (2025). An analysis of cybersecurity culture among the Nigerian academia. *Kontagora International Journal of Educational Research (KIJER), 2*(2), 231–249

DOI: https://doi.org/10.5281/zenodo.15103811

Abstract

The aim of this study was to quantitatively analyse the notion of cybersecurity culture among the Nigerian academia in North Central Nigeria. The study sought the perception among the students, academic and administrative staff of the different institutions of higher learning in Nigeria on the existence of cybersecurity culture and information security awareness. The quantitative research adopted a homogeneous sampling method, a procedure of choosing participants with parallel traits was used to select 327 participate from eighteen Nigerian tertiary institutions based in the North-Central region of the country. The data was collected to obtain the level of awareness, perception and behavioural traits through the use of an online questionnaire survey tool utilising a five-point Likert scale. Data collected was analysed by comparison of means, Analysis of Variance (ANOVA) and Chi-Square statistics at .05 level of significance using the Statistical Package for the Social Sciences (SPSS) IBM version 20.00. The findings of this research showed that the level of awareness of cybersecurity was very low and the perceived existence of a cybersecurity culture was also weak in the different levels of tertiary educational institutions in North-central Nigeria. It was also found that the behavioural traits of individuals and administrators in the system were not those that will encourage a strong cybersecurity culture in the Nigerian academia. From the responses it was also clear that the management of institutions did not prioritise information security, practices, policies and procedures as a practice in their institutions. The paper recommends that the Nigeria tertiary institutions should enhance their information security culture by implementing comprehensive awareness programs, strengthening policies, prioritizing cybersecurity governance, investing in advanced security infrastructure, fostering security ownership, and promoting research and collaboration to mitigate data breaches and protect sensitive information

Keywords: *Cybersecurity culture, information security awareness, information security perception, Education, North-Central region*

Introduction

Advancement in network infrastructure and information system has been extensively discussed by researchers and practitioners alike. In the modern day, this has doubtlessly revolutionized the way information is been processed, stored, shared and communicated between people, businesses, organizations, and government (Wasserbauer, 2023; Fyfield et al., 2022; Alfawaz, 2015; Clausen, 2010; Hentea et al., 2006). In the new global economy and today's information age; cyberspace, a creation of the internet has provided a dynamic platform for socio economic development and globalization, existences of diverse vulnerabilities within its system had made cyber threat popularity attain the status of daredevil Hollywood superstars. However, Da Veiga et al. (2020) suggested that to address the growing cyber-attack and security breaches it is important to better understand the information security culture of an organization. For this research, Information Security and Cybersecurity will be used interchangeably as their terms are very closely related terms. Oforji et al., (2017) define Cyber Security as the ability to protect or defend the use of cyberspace from cyber-attacks. Whereas, Information Security is broader and deals with the protection of information whether be it physical or computerized (Alfawaz & Nelson, 2010).

Today researchers agree that information security culture is now becoming a key element for organizations. Information security culture is defined as the set of qualities, shared by everybody in an association, which decide how individuals are required to consider and approach security in the system (da Veiga et al., 2020; Alhogail, 2015). However, Hentea et al (2006) defined it as the gathering of insights, conducts, values, expectations, and information that directs the human communication with data properties in a firm with the ultimate goal of manipulating workers‟ security demeanour. Information security culture emergence relies on ensuring that members of an organization are mindful of data security in their everyday occupational routine. Tang et al., (2016) stated that achieving a functional security culture depends on the organization information security policy perception of system users and how important the organization information safety means to them. Information security is vital to unravelling the effectiveness of on-going security awareness (Pahnila et al., 2007) and the rationales behinds non-compliance of some academia to information security-related activities and cultures. Effective information security is vital to ensure that staff understands and are committed to information security management programmes such as securing password best practice, phishing

detection and avoidance, regular updating of anti-malware program and policy reading and compliance throughout the institution.

Therefore, this research will focus on the analysis of information security culture among the Nigerian academia. The study will focus on the notions of information security culture of lecturers, students, and non-academic staff of selected universities in the northern region of Nigeria with the aim of understanding the ideas, norms, attitudes, and behaviours towards compliance and adoption of organization information security culture. The understanding of the opinion of the end user's perception and attitudes toward their institutions' information security culture is relevant to understanding the rationale behind risky security behaviour and how best to reduce vulnerabilities related to it. Limitations of the research would be addressed and finally, the inferences for information security management approach in Nigeria and future research are discussed

Statement of Problem

The increasing reliance on computers and the internet in Nigerian tertiary institutions has led to the adoption of cloud technologies for security and innovation. However, challenges persist in effectively managing information technology, particularly in fostering a cybersecurity culture within educational institutions. While cybercrime remains a global concern, Nigeria ranks third in cyber-related offenses, with many university students reportedly engaging in fraudulent activities such as "Yahoo plus" (Ogundele et al., 2023). These activities not only pose threats to individuals but also compromise institutional information systems. Despite growing cybersecurity threats, many end-users in Nigeria exhibit limited awareness of security risks, often perceiving threats as limited to viruses and phishing scams. Additionally, existing awareness campaigns have proven ineffective, as many individuals operate based on personal beliefs rather than institutional cybersecurity policies (Garba et al., 2021). Factors such as ignorance, poverty, and cultural perceptions further contribute to users' vulnerability to cyber threats, highlighting the need for a deeper understanding of cybersecurity attitudes and behaviors in Nigerian tertiary institutions (Information Security Forum (ISF), 2016).

There is a notable gap in literature concerning information security culture within Nigerian higher education institutions, with limited studies examining the effectiveness of security management frameworks compared to Western nations. This study seeks to bridge this gap by applying Schein's (1985) organizational culture theory to analyze security-related behaviors among lecturers, students,

and non-academic staff in selected Nigerian universities, polytechnics, and colleges of education. By assessing perceptions, attitudes, and compliance with information security policies, the research aims to provide insights into the existing cybersecurity culture and explore ways to enhance security awareness and adoption. Given the contextual and cultural differences between Nigeria and Western countries, this study will offer a localized perspective on the challenges and opportunities in building a sustainable information security culture within Nigerian tertiary institutions.

Research Aim and Objectives

The aim of this study is to quantitatively analyze the notion of cybersecurity culture among the Nigerian academia in North Central Nigeria with the following objectives:

1. To determine the existence of information security culture and the related practices in different institutions of higher learning in Nigeria.
2. To assess the level of information security awareness amongst the students, teaching, and non-teaching staff of the different institutions.
3. To analyze the perception of the students, teaching, and non-teaching staff regarding cybersecurity culture

Research Questions

The following research questions were considered:

1. What level of awareness do students and staff have of their institution's cybersecurity culture?
2. What perceptions do students and staff have of their institution's cybersecurity culture?
3. What factors influence the weakness, strength or absence of security culture in these organisations?

Hypothesis

In order to determine the level of awareness, existence and strength of cybersecurity culture and related practices in the different institutions in the Nigerian academia, and further make valid inferences on the set research questions, three hypotheses were developed:

i. There is no significant adoption of cybersecurity culture and related practices in higher education institutions in Nigeria.

ii. There is no significant difference in the level of awareness of cybersecurity culture in different institutions in the Nigerian Academia.

iii. There is no significant difference in the perception of different institutions on cybersecurity culture in the Nigerian Academia

Methodology

This study adopts a quantitative research methodology, aligning with a positivist epistemology and deductive approach to investigate cybersecurity culture in Nigerian academia. A survey method was used to collect factual data, ensuring objective measurement of cybersecurity awareness, perception, and behavioral influences. categorized into cybersecurity awareness, compliance, and attitudinal factors. The primary research instrument was a structured questionnaire, which included a section on demographic information and 39 Likert-scale items. These items were systematically categorized into three key areas: cybersecurity awareness, compliance with security policies, and attitudinal factors influencing cybersecurity practices.

The study targeted academic staff, administrative personnel, and students across 18 tertiary institutions in North-Central Nigeria. A homogeneous sampling technique was employed, selecting participants with knowledge of cybersecurity, yielding a final sample of 327 respondents. The survey was distributed via email, telephone, and social media, with data collected through the Smart Survey platform.

The primary data collection instrument for this study was a structured questionnaire, systematically designed to obtain relevant information from respondents. The questionnaire was organized into two distinct sections to ensure a comprehensive approach to data gathering. Section A focused on collecting demographic data and included a consent form to secure informed participation. Section B comprised 39 carefully formulated items designed to elicit responses using a five-point Likert scale, ranging from Strongly Disagree to Strongly Agree. The items in this section were categorized into three key thematic areas.

The first category assessed respondents' perspectives on cybersecurity culture and their awareness of security policies within Nigerian academia. The second category examined perceptions of and adherence to cybersecurity policies in academic institutions. The third category explored the behavioral and attitudinal factors influencing security culture in Nigerian academia. This structured approach facilitated a rigorous examination of cybersecurity-related issues within the academic sector, ensuring the reliability and validity of the data collected

To ensure the reliability and validity of the research instrument, a pilot study was conducted prior to full-scale data collection. The instrument was evaluated by cybersecurity experts and academic researchers to assess its relevance, clarity, and comprehensiveness. Internal consistency was examined using Cronbach's Alpha, yielding a reliability coefficient of 0.81. Based on feedback from both experts and pilot study participants, necessary modifications were made to enhance the clarity, validity, and overall effectiveness of the questionnaire."

The questionnaire was administered through an online survey tool, SmartSurvey which facilitated efficient data collection. The survey link was distributed via email, telephone, and social media platforms such as WhatsApp and Facebook. Prior to distribution, potential respondents were contacted and briefed on the purpose of the research. Participants were assured of anonymity and confidentiality to encourage honest responses.

The collected data were analyzed using the Statistical Package for the Social Sciences (SPSS), IBM Version 20. Descriptive statistics, including mean values and frequency distributions, were employed to summarize the data effectively. To ensure a comprehensive and rigorous analysis, various statistical techniques were utilized. A comparison of means was conducted to examine differences in perceptions across various groups of respondents. Analysis of Variance (ANOVA) was applied to assess multiple independent variables and determine statistically significant differences among groups. Additionally, the Chi-Square test was employed to evaluate relationships between categorical variables. These analytical methods provided robust insights into the dataset, ensuring the validity and reliability of the findings.

Data Analysis and Results

A questionnaire survey was conducted across 18 tertiary institutions in North Central Nigeria, with 350 invitations sent via email and webmail. A total of 332 responses were completed online, and after excluding five incomplete ones, 327 valid responses (93.4%) were analyzed. Respondents represented diverse backgrounds, education levels, and occupations, with 37% from universities, 39.9% from colleges of education and 32.1% from Polytechnics. The occupational distribution included 32.1% students, 35.5% academic staff, and 32.4% administrative staff.

Research Question 1 • What is the level of awareness of students and staff in their institution's Cybersecurity culture?

For the first item in Table 1, the mean responses of the occupational groups (students, Academic and Administrative) ranged from 3.33 - 3.48. It is evident from the result that many of the respondents did not know whether their institutions had an information security awareness programme. In Items 8 and 9 the students and academic staff had mean values between 2.49-2.92 which imply that they disagreed with participating and or learning any information security skills from their institutional cybersecurity awareness programmes. Most respondents in the administrative cadre had mean values of 3.00 and 3.08 for the items. This shows wherein different on whether or not they have actively participated in cybersecurity awareness programmes or have learnt skills in the area. In items 10 and 12, all the respondents claimed they did not know whether they have been discussing issues of cybersecurity safety with colleagues and that they were not aware of the procedures for reporting cybersecurity issues in their institutions.

Table 1

Responses from participants

Items		Students	Academic Staff	Administrative staff
7. My institution has an information security awareness programme	Mean	3.33	3.41	3.48
	SD	1.03	1.11	1.01
8. I have been an active participant in the information security awareness programme my institution	Mean	2.52	2.75	3.00
	SD	1.13	1.24	1.13
9. My information security skills were learned from the awareness and training programmes organized by my institution	Mean	2.49	2.92	3.08
	SD	1.18	1.18	1.19
10. I discuss information security safety issues with my colleagues	Mean	3.27	3.27	3.21
	SD	1.20	1.15	1.15
12. I am aware of the procedures for reporting security policy violations in my institution	Mean	2.69	3.15	3.29
	SD	1.30	1.35	1.10

Table 2

General level of Awareness of the different Cadre

Awareness				
Cadre	Mean	N	Std. Deviation	% of Total Sum
Student	2.9810	105	.98284	30.9%
Academic	3.0474	116	1.04044	34.9%
Administrative	3.2689	106	.96898	34.2%
Total	3.0979	327	1.00363	100.0%

In general, from table 2, the mean responses among the three occupational groups is 2.98, 3.05 and 3.27. The students had the lowest level of awareness as opposed to the administrative group which usually form to first contact group when policies are disseminated in a tertiary institution in Nigeria

Table 3

Level of Awareness among different Institutions

Awareness				
Institution	Mean	N	Std. Deviation	% of Total Sum
University	3.3306	121	.94550	39.8%
College of Education	2.7921	101	1.03264	27.9%
Polytechnic	3.1394	104	.96405	32.3%
Total	3.1028	326	1.00124	100.0%

From table 3, The universities had the highest mean of 3.33 with colleges of Education having the lowest mean of 2.79 this indicates that the members of the university community have shown a higher level of awareness on cybersecurity issues. In general the level of awareness of the Nigerian Academia on cybersecurity culture is very low.

Research Question 2 : What perceptions do students and staff have of their institution's cybersecurity culture?

Table 4

Responses on the perception of institutions on Cybersecurity culture

Items		University	Colleges of Education	Polytechnics
15. The institution insists that we use licensed software (such as Microsoft Office) in computers supplied by the institution	Mean SD	2.93 1.23	2.79 1.21	2.58 1.16
16.The management check compliance with licensed software and use of originally licensed antivirus in my institution	Mean SD	2.79 1.16	2.43 1.15	2.57 1.09
17. I hardly use licensed software and antivirus on my computers due to financial challenges	Mean SD	3.09 1.32	3.03 1.29	2.68 1.04
18. In my institution, computer operating systems (such as Windows) are upgraded every year	Mean SD	2.93 1.08	2.59 1.09	2.69 1.03
22. There is an information security policy in my institution	Mean SD	3.32 1.02	2.78 1.05	2.99 1.04
23. I am free to ask questions about problems relating to information security (e.g virus, hacking, password challenge…)	Mean SD	3.41 1.15	2.74 1.17	2.94 1.11
24. The importance of information security is clearly communicated by management	Mean SD	3.02 1.14	2.27 1.04	2.80 1.15
27. Information security expectations are clearly defined and communicated by my institution	Mean SD	3.27 1.01	2.51 1.11	2.83 1.17
29. My institution has a written information security policy and/or strategy	Mean SD	3.21 0.96	2.60 1.14	2.69 1.11

To answer this question, items 15,16,17,18,22,23,24,27 and 29 were used. The perception of students and staff of cybersecurity in different levels of tertiary education in North-Central Nigeria is analysed and presented in table 4. From the results, the perception of cybersecurity was measured using the practices that culminate in the security culture of any institution that has a well spelt out security culture. In items 15,16, and 18, the respondents in all the tiers of tertiary education disagreed that the institutions insisted on the use of licensed software and that the management checks compliance with license and use of original antivirus software and that such software was not usually updated yearly.

Research Question 3: What factors influence the weakness, strength or absence of security culture in these organisations?

Table 5

Behavioural/Attitudinal factors affecting cybersecurity culture

Items		University	Colleges of Education	Polytechnics
33. Management make themselves approachable and allow effective two-way communication	Mean	3.12	2.63	2.84
	SD	1.12	1.16	1.02
34. Management launch, if necessary, procedures for investigating security problems, seeking advice	Mean	3.32	2.43	2.57
	SD	0.97	1.15	1.09
35. The institution administration provides fair treatment of subordinates, understanding that errors	Mean	3.09	2.84	3.06
	SD	1.32	0.97	0.93
36. Management involve staff members in the risk assessment and decision making processes	Mean	3.38	2.78	2.78
	SD	0.93	0.97	0.87
37. Management encourage, recognize and reward commendable attitudes	Mean	3.28	2.66	2.73
	SD	1.08	1.01	0.97
42. I am more likely to break rules due to management pressure	Mean	2.84	2.78	2.61
	SD	1.14	0.96	0.88
43. I am more likely to bend rules due to management pressure	Mean	3.07	3.23	2.81
	SD	1.19	1.13	0.96
45. Staff members seek guidance when unsure of the security significance of the unusual event	Mean	3.33	2.93	2.84
	SD	0.94	0.91	0.93

To answer this question, item 33 to 46 were used. The results shown in Table 5 indicate that the behavioural/attitudinal traits that contribute to a strong cybersecurity cultures stem from the authorities handling such issues and the end users. Items 33-37 deals with the management of institution's attitude to enhancing a strong cybersecurity culture. In the tiers of tertiary education in the Northcentral Nigeria, the members of the Colleges of Education and Polytechnic communities had means ranging from 2.43-2.84. This indicates that the management was not approachable to enhance effective communication, could not launch appropriate measures to seek solutions to problems of information security when they arise; the administrators did not render fair treatment of subordinates. Worst still, little or no

encouragement, or recognition and reward commendable attitudes that will promote cybersecurity culture in the Nigerian academia in North-central Nigeria. The university communities had higher mean values ranging from 3.07 to 3.38. this also implies that such attitudes that will encourage a good security culture were lacking in the Northcentral universities.

Hypotheses

H_{01}: There is no significant adoption of cybersecurity culture and related practices in higher education institutions in Nigeria.

Table 6

Chi-Square Test Results for Assessing Cybersecurity Culture

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	36.251[a]	16	.003
Likelihood Ratio	39.681	16	.001
Linear-by-Linear Association	10.086	1	.001
N of Valid Cases	327		

a. 14 cells (51.9%) have expected count less than 5. The minimum expected count is .31.

From table 6, the results revealed a statistically significant association (**$p = 0.003$, $p < 0.05$**), indicating that cybersecurity culture and practices are present in these institutions. Further analysis using symmetric measures showed that Phi (**0.333**) and Cramer's V (**0.235**) values suggest a **moderate to weak-moderate relationship**, respectively. While the association is statistically significant, the strength of the relationship indicates that the presence and implementation of cybersecurity culture and related practices vary across institutions

H_{02}: There is no significant difference in the level of cybersecurity awareness across institutions in Nigerian academia.

Table 7

ANOVA in Cybersecurity Awareness Scores Results Across Institutions

Awareness					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	16.068	2	8.034	8.335	.000
Within Groups	312.301	324	.964		
Total	328.369	326			

Table 7 results indicated that the variance in cybersecurity awareness scores across institutions was not significantly different ($p = 0.168$, $p > 0.05$). As the assumption of homogeneity was met, a one-way analysis of variance (ANOVA) was deemed appropriate for further analysis. The results of the ANOVA revealed a statistically significant difference in the level of cybersecurity awareness among institutions, as indicated by an F-statistic of 8.335 and a p-value of 0.000 ($p < 0.05$). Consequently, the null hypothesis was rejected in favor of the alternative hypothesis, suggesting that awareness levels of cybersecurity culture vary significantly across institutions.

Further analysis comparing Colleges of Education, Polytechnics, and Universities showed that Colleges of Education ($M = 2.7921$) and Universities ($M = 3.3306$) belonged to distinct subsets, indicating a significant difference in awareness levels between these institutions. In contrast, Polytechnics ($M = 3.1238$) overlapped with Universities in one subset, suggesting that their awareness levels were more closely aligned with those of Universities than with Colleges of Education. The significance value for institutions within the same subset was 1.000, confirming that there were no significant differences within subsets, while institutions in different subsets exhibited statistically significant variations in cybersecurity awareness. Based on these findings, H_{02} was rejected, supporting the conclusion that cybersecurity awareness levels differ significantly across institutions in Nigerian academia

H_{03}: There is no significant difference in the perception of cybersecurity culture across institutions in Nigerian academia.

A test of homogeneity of variances was conducted to determine whether the assumption of equal variances was met. The results indicated that variance in perception scores across institutions was not

significantly different (**p = 0.263, p > 0.05**), confirming that the assumption of homogeneity was satisfied. Therefore, a one-way analysis of variance (ANOVA) was conducted to examine differences in the perception of cybersecurity culture among institutions.

Table 8

ANOVA Results in Cybersecurity Culture Perception Among Institutions

Perception					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	22.208	2	11.104	13.458	.000
Within	267.321	324	.825		
Groups					
Total	289.529	326			

The ANOVA results revealed in table 8, indicated a statistically significant difference in cybersecurity culture perception among institutions (**F = 13.458, p = 0.000, p < 0.05**). As the p-value was below the significance threshold, the null hypothesis (**H_{03}**) was **rejected**, confirming that perceptions of cybersecurity culture vary significantly across institutions. Further post hoc analysis comparing Universities, Polytechnics, and Colleges of Education revealed significant differences in mean values. A notable mean difference of 0.62589 (p = 0.000) was observed between Universities and Colleges of Education, indicating a substantial variation in their responses. Similarly, a significant mean difference of 0.37973 (p = 0.005) was found between Universities and Polytechnics. However, no significant difference was detected between Polytechnics and Colleges of Education (p = 0.128), suggesting that these two institutions share similar perceptions.

These findings suggest that Universities perceive cybersecurity culture significantly differently from both Colleges of Education and Polytechnics (p < 0.05). However, there was no significant difference in perception between Polytechnics and Colleges of Education (p = 0.128). Mean perception scores indicate that Universities had the highest perception (M = 3.2893), followed by Polytechnics (M = 2.9095), while Colleges of Education had the lowest perception (M = 2.6634).

Discussion

The major findings of this study indicated a relationship to the objectives and research questions of the study relating to the concept of information security culture in the Nigerian Academia. The assessment identified that these include the involvement of top administrators, policy implementation, policy maintenance, moral conduct policies, and information security training. In essence, this means that Nigeria's higher institutions generally experience a weak system when dealing with information security culture. It also means that these institutions did not prioritize information security in their organization.

The results of the study also provided that information security culture in Nigeria consists of three essential concepts including awareness of information security policies, information security policy adherence, and security ownership. These findings are important because they will help other institutions to devise better ways of safeguarding their information. They can also be related to similar investigations conducted earlier, for example, Garba et al., (2021) and Odumesi (2014) who asserted that adherence to information security policies is vital to business success over the digital network. Alternatively, Alfawaz (2015) observed that information security policy adherence provides for privacy and ethical access to information concerning a given organization. With this investigation, it was determined that most participants were aware of the risks involved in the failure to comply with information security policies. In fact, it was discovered that most people only find challenges in cases where they are unaware of the procedures for reporting violations of information security policies. To this, several previous kinds of literature agree including Alfawaz and Nelson (2010) who posited that information security policy awareness allows for efficient security of information. This means that most tertiary institutions in Nigeria need to care about information security awareness and training and also allocate sufficient financial resources towards the training of staff members and students about the security of their information which constitute cybersecurity culture. This can be related to prior studies by da Veiga et al., (2020) who noted that corporations should ensure that an information security culture is adequately defined by educating and training employees toward improved awareness of information security.

According to Amujiri and Agu (2012), investing in cyber security tools, training, policies, procedures, and risk management can potentially assist in safeguarding the information of a given

organization. Also, Da Veiga and Eloff (2010) observed that training employees toward improved awareness of information security guarantee a reduction in the hazards of information resources. From this assessment, it has been identified that Nigerian higher education institutions do not take it crucial to improve and communicate risky conduct and policies to all staff members. Primarily, the appropriate ethical behaviour is necessary if institutions are to safeguard their sensitive data. This relates to prior analyses such as Collard et al.,(2024) and Alhogail (2015) which postulate that morality and accessibility of information can be effectively achieved through encouraging appropriate ethical behaviour among staff members. Basing on the first objective of the study, it was discovered that there is an existence of a weak cybersecurity culture in the Nigerian Academia. Several higher-level institutions have not recognized information security and directed frantic efforts towards safeguarding their sensitive data. This is in line with a study by Ogundele et al., (2023) which revealed that students in South-Western Nigerian had low information security awareness.

For objective number two, it was determined that there is a low level of awareness regarding information security among Nigeria's higher institutions of learning. In addition, the maximum awareness level score was the awareness of the risk of not complying with information security policies. Ogundele et al., (2023) and Abolarinwa et al. (2015) highlight that the need for enhancing visibility, encouraging, reporting, promoting awareness of cybersecurity especially in the tertiary education system in Nigeria.

For the third objective, this assessment revealed that the respondents in Nigeria's tertiary institutions were of the view that management did not regard information security to be a priority. Sutton and Tompson (2025) asserted that achieving a functional security culture depends on the organization's information security policy perception of system users and how important the organization information safety is of value to them. The results of this examination have significantly exhibited the necessity to improve information security culture through policies in Nigeria's higher institutions of learning. As observed in this discussion, they also agree with prior literature concerning this topic. Finally, this assessment contributes to the existing research with its results about the influencing factors of information security breaches in the Nigerian tertiary education sector

Conclusions

The level of awareness on cybersecurity culture in North-Central Academia was observed to be very low and the perceived cybersecurity culture was weak. Also behavioural traits of individuals and administers in the system were not those that will encourage a strong cybersecurity culture in the Nigerian academia. It was also found that the management of institutions did not prioritize information security, practices, policies and procedures, as well as technology. Previous research suggests that human behaviour influences the management of information security culture. This given analysis has discovered that the establishment of a security culture is important and inevitable for tertiary institutions to boost the efficiency engrossed in running their information security systems. Several factors including the involvement of top administrations, policy implementation, policy maintenance, policies of moral conduct and security training greatly contribute to this effectiveness. One of the most significant aspects of the findings of this assessment is that they prove to be relatable to prior investigations. In particular, these stipulate that there is a close relationship between the safety of an institution's sensitive information and its subsequent effective operations. For that reason, higher level institutions are advised to boost information security in a bid to intercept data breaches. For this analysis, it was found that information security culture in Nigeria consists of three essential concepts including information security policy awareness, security policy adherence, as well as security ownership. It also revealed that Nigerian higher level education institutions exhibit weak information security ownership. There is, therefore a need for institutions to review the awareness programs relating to information security to ensure that their sensitive data is protected from breaches.

The challenges and significance of this study exceed the identification of information security culture as a primary information security management issue in Nigeria's higher institutions of learning. Essentially, the significance of this current evaluation is being able to comprehend what constitutes an information security culture. The critical aspects that tend to impact information security culture were examined including the early understanding of the link between these factors and those that constitute or reflect security culture. The analysis developed a reliable and valid information security culture measurement theory as the primary contribution to the existing research in this area. Ideally, institutions ought to develop effective information security cultures to safeguard sensitive data concerning the students and staff members. This can be realized through the establishment of data security policies to

govern and control the dissemination of information among the staff members and students which form the academic community of tertiary institutions in Nigeria.

Recommendations

1. Higher education institution in Nigeria should establish structured cybersecurity awareness programs to educate staff and students on the significance of information security policies and best practices.
2. Institutions should develop, implement, and periodically review comprehensive cybersecurity policies that define roles, responsibilities, and acceptable security practices.
3. Tertiary institutions' administrators and policymakers must prioritize cybersecurity as a strategic objective by allocating adequate financial and human resources for information security initiatives.
4. To enhance information security culture, Nigerian education institutions should cultivate a sense of security ownership among staff and students by promoting proactive engagement with security policies.
5. Tertiary institutions should actively engage in cybersecurity research to identify emerging threats and develop innovative security solutions tailored to the academic environment.

References

Alfawaz, S. M. (2015). Information security management : A case study of an information security culture. *Journal of Research and Practice in Information Technology*, *2*(3), 36–45. http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCIQFjAA&url=http://eprints.qut.edu.au/41777/1/Salahuddin_Alfawaz_Thesis.pdf&ei=806tU6-XA6ad0QWloIAY&usg=AFQjCNGIpB_BnZeCNvuateNiTRyNXWRdvg&sig2=grUx8GqTlSFXp

Alfawaz, S., & Nelson, K. (2010). Information security culture : A Behaviour Compliance Conceptual Framework. *Australasian Information Security Conference*, *105*(Aisc).

Clausen, L. (2010). Moving beyond stereotypes in managing cultural difference: Communication in Danish-Japanese corporate relationships. *Scandinavian Journal of Management*. https://doi.org/10.1016/j.scaman.2009.11.008

Collard, A., Kraemer, M. J., & Smothers, R. L. (2024). *CULTURE 2024*.

da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational

information security culture—Perspectives from academia and industry. *Computers & Security*, *92*, 101713. https://doi.org/10.1016/j.cose.2020.101713

Fyfield, M., Henderson, M., & Phillips, M. (2022). Improving instructional video design: A systematic review. *Australasian Journal of Educational Technology*, *38*(3), 155–183. https://doi.org/10.14742/ajet.7296

Garba, A. A., Siraj, M. M., Othman, S. H., & Zogaan, W. A. (2021). Cybersecurity Awareness of University Students in Nigeria: Analysis Approach. *Turkish Journal of Computer and Mathematics Education*, *12*(12), 3739–3752.

Hentea, M., Dhillon, H. S., & Dhillon, M. (2006). Towards Changes in Information Security Education. *Journal of Information Technology Education*, *5*, 221–233.

Information Security Forum (ISF). (2016). The Standard of Good Practice for Information. In *Information Security Forum Limited*.

Odumesi, J. O. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology*. https://doi.org/10.5897/IJSA2013.0510

Oforji, J. C., Udensi, E. J., & Kelechi, I. (2017). CYBERSECURITY CHALLENGES IN NIGERIA: THE WAY FORWARD. *SosPoly Journal of Science & Agriculture*.

Ogundele, A. T., Awodiran, M. A., Idem, U. J., & Anwana, E. O. (2023). Cybercrime Activities and the Emergence of Yahoo Boys in Nigeria. *2023 International Conference On Cyber Management And Engineering (CyMaEn)*, 313–320. https://doi.org/10.1109/CyMaEn57228.2023.10051083

Pahnila, S., Siponen, M., Mahmood, A., Box, P. O., Oulun, F.-, & Siponen, E. M. (2007). Employees ' Behavior towar ds IS Secur ity Policy Compliance University of Oulu , Department of Information Processing. *October*, 1–10.

Sutton, A., & Tompson, L. (2025). Towards a cybersecurity culture-behaviour framework: A rapid evidence review. *Computers and Security*, *148*(July 2024), 104110. https://doi.org/10.1016/j.cose.2024.104110

Tang, M., Li, M., & Zhang, T. (2016). The impacts of organizational culture on information security culture: a case study. *Information Technology and Management*, *17*(2), 179–186. https://doi.org/10.1007/s10799-015-0252-2

Wasserbauer, M. (2023). *The Effect of Information Technology Infrastructure and the Internet of Things on Defense Industry Management Information Systems*. *4*(1), 190–200.