International Journal of Innovative Social Sciences & Humanities Research 12(1):227-241, Jan.-Mar., 2024

© SEAHI PUBLICATIONS, 2024 www.seahipublications.org ISSN: 2354-2926

Assessment of Cyber Counter-Intelligence Awareness and Practices among Students in Universities in Rivers State, Nigeria

Nwokoro, C. O., Obinnachi C., Nath, M. A and Nwogu, U. J.

Department of Education Management,
Faculty of Education,
University of Port-Harcourt, Port-Harcourt, Nigeria

ABSTRACT
This study investigated the Assessment of Cyber Counter-Intelligence Awareness and Practices among Students in Universities in Rivers State, Nigeria. The study was guided by three research questions and three null hypotheses, employing a descriptive survey design. The research focused on a population of 900 undergraduate students selected from three public tertiary institutions in Rivers State, namely University of Port-Harcourt, Rivers State University and Ignatius Ajuru University of Education, a multistage sampling procedure was adopted for sample and sampling techniques. Data collection involved the use of a validated 30-item questionnaire titled the Assessment of Cyber Counter-Intelligence Awareness and Practices among Students in Universities in Rivers State Questionnaire with a reliability index of 0.86 established through Cronbach method. Research questions were addressed using mean values, while hypotheses were tested employing the z-test. Findings indicate that although users have the right to provide protection against foreign intelligence operations, cyber counter-intelligence is under-utilized. Moreover, actions are taken to identify and counter adversary intrusions, scholars have swift access to current information on cyber counter-intelligence, and maintenance access is provided to enhance penetration testing. However, students' usage of cyberspace for cyber counter-intelligence is low. Recognizing these challenges, the study advocates for targeted strategies to bridge the knowledge-practice gap in cybersecurity among undergraduate students. Recommendations include prioritizing comprehensive cybersecurity awareness programs in educational institutions, focusing on issues such as password security, email management, and data backup processes. Furthermore, students should be educated on vulnerability assessment to enhance their cyber space usage. The study acknowledges its limitations and suggests avenues for future research.
Keywords: Cyber Counter-Intelligence, Practices, vulnerability assessment, Undergraduate Students.

INTRODUCTION

In the contemporary era, safeguarding valuable assets takes on diverse forms, extending beyond the protection of tangible elements like life and property. In education, especially within the dynamic landscape of universities in Rivers State, Nigeria, the focus on safeguarding extends to the preservation of digital assets. The academic milieu, characterized by copious volumes of critical information such as student records, enrolment details, and academic outcomes, demands a robust defence mechanism to ensure the seamless functioning of the educational system. As the educational landscape undergoes a

paradigm shift with the integration of Information and Communication Technology (ICT), the need to fortify the digital frontier becomes increasingly imperative (Federal Republic of Nigeria, 2004; Nwokoro, 2017).

The advent of ICT in education has given rise to electronic learning (e-learning), transforming traditional teaching methods into online platforms where both teaching and learning activities are conducted virtually. Concurrently, the management of records, communication, and information transfer has transitioned from manual processes to electronic systems (Baniulyte et al., 2023; Beierle et al. 2023 & Flemming & Hübner, 2013). While developed countries have fully embraced ICT in education, employing various communication technologies, ranging from standalone systems to internet-connected networks, the increased reliance on cyberspace introduces new challenges and security considerations.

Cyberspace, an intricate online world of interconnected computer networks facilitated by the internet, mirrors the physical world but offers unparalleled convenience and opportunities. It encompasses diverse activities, ranging from cyber journalism, governance, politics, evangelism, broadcasting, socialization, and commerce to cybersecurity threats like cyberbullying, cyberstalking, and cybercrime (Jamshidi et al., 2023, Ashraf, et al., 2023, Sarkar & Shukla, 2023 & Riega-Virú et al., 2023). As the educational sector embraces the benefits of cyberspace, it concurrently grapples with the security challenges posed by cybercrime.

Cybercrime, inherently linked to criminal activities utilizing computers or networked systems, necessitates comprehensive cybersecurity measures to safeguard internet-connected systems, including hardware, software, and data. In the quest for enhanced cybersecurity, the introduction of Cyber Counter-Intelligence (CCI) emerges as a strategic imperative. CCI encompasses measures designed to identify, penetrate, or neutralize foreign operations employing cyber means as their primary methodology. These measures extend beyond traditional intelligence service methods, evaluating both cyber capabilities and intentions (Duvenage & Von Solms, 2013).

In the educational landscape, where information and communication technologies are integral to teaching and learning, CCI becomes essential to ensure the proper dissemination and efficient management of information within cyberspace.

Within Rivers State, three public universities—the University of Port-Harcourt, Rivers State University, and Ignatius Ajuru University of Education—have embraced ICT, with internet-connected computers facilitating access to information, bridging communication gaps, and enabling virtual learning experiences. This exposure to cyberspace necessitates a conscientious application of Cyber Counter-Intelligence within the tertiary education system. Consequently, this study endeavours to assess the extent to which students engage in practices aimed at ensuring the effective management of Cyber Counter-Intelligence within universities in Rivers State.

Statement of the Problem

The infusion of Information and Communication Technology (ICT) has ushered in transformative shifts, redefining traditional teaching practices and administrative functions while serving as a catalyst for growth in the global economy and the educational sector. The transition from chalk and face-to-face interactions to digital platforms such as magnetic boards, Google Classroom, Docebo, Wiziq, Adobe Captivate, and virtual classrooms has created a new paradigm where teachers and learners communicate through mobile and internet connections in cyberspace. While this evolution brings efficiency and convenience, it concurrently exposes educational institutions to various cyber threats, necessitating a vigilant approach to cybersecurity (Federal Republic of Nigeria, 2004; Nwokoro, 2016).

In the wake of continuous access to computers, the heightened reliance on cyberspace amplifies vulnerabilities to various threats, including computer viruses, ransomware, data leakage, phishing, and hacking. Amidst the global shift towards virtual education, the relevance of Information Technology (IT) security is paramount, mainly as post-secondary schools actively engage in cyberspace to sustain academic work during the Coronavirus (COVID-19) pandemic era. Cybercrimes, ranging from email and internet fraud to identity theft, financial data theft, and cyber espionage, underscore the critical need for

heightened awareness and security measures within educational institutions (Andini et al., 2023 & Kala, 2023).

As lecturers and students navigate the intricacies of cyberspace; the threat of unauthorized access, intrusion, and hacking looms large. Hacking activities have become a daily occurrence, necessitating proactive measures to protect computer systems from unauthorized access, especially with the integration of sophisticated IT facilities to meet the evolving needs of the educational system. Against this backdrop, the central question that propels this study is: To what extent are students engaged in practices that ensure the effective management of cyber counter-intelligence in universities in Rivers State? This question encapsulates the imperative to assess students' awareness and proactive measures to safeguard against cyber threats within the educational environment, aiming to unravel the dynamics of Cyber Counter-Intelligence awareness and practices in universities in Rivers State, Nigeria.

Aim and Objectives

The aim of this study was to assess the Cyber Counter-Intelligence Awareness and Practices among Students in Universities in Rivers State. The study sought to:

1. Ascertain the level of awareness in the management of cyber counter-intelligence among students of universities in Rivers State.
2. Find out the level of adoption of penetration testing practices in the management of cyber counter-intelligence among students in universities in Rivers State.
3. Ascertain the extent to which vulnerability assessment is adopted in the management of cyber counter-intelligence among students in the universities in Rivers State.

Research Questions

In addressing the problem of this study, the following research questions were posed to guide the study:

1. What is the level of awareness in the management of cyber counter-intelligence among students of universities in Rivers State?
2. What is the level of adoption of penetration testing practices in the management of cyber counter-intelligence among students in universities in Rivers State?
3. What is the extent to which vulnerability assessment is adopted in the management of cyber counter-intelligence among students in the universities in Rivers State?

Hypotheses

The following null hypotheses were postulated and tested at 0.05 level of significance

1. There is no significant difference between the mean ratings of male and female students on the level of their awareness in the management of cyber counter-intelligence in universities in Rivers State;
2. There is no significant difference between the mean ratings of male and female students on the level of adoption of penetration testing practices in the management of cyber counter-intelligence in universities in Rivers State;
3. There is no significant difference between the mean ratings of male and female students on the extent to which vulnerability assessment is adopted in the management of cyber counter-intelligence in the universities in Rivers State.

METHODOLOGY

This study adopted a descriptive survey design. The population comprised one thousand (900) male and female student. .A multistage sampling procedures was drawn for sample and sampling technique and obtain a sample of four hundred and four (404) Male and four hundred and ninety six (496) female from three public universities in Rivers State namely University of Port Harcourt, the Rivers State University and the Ignatius Ajuru University of Education. Instrument used for data collection was a 30 item questionnaire tagged – **Assessment of Cyber Counter-Intelligence Awareness and Practices among Students in Universities in Rivers State, Nigeria (ACCIAPSURSN)**. It was patterned after the Likert (Modified) response scale with four options (Very High Level, High Level, Low Level and Very Low Level and Very High Extent, High Extent, Low Extent, Very Low Extent). The instrument was duly validated by three experts in instrumentation and measurement department. It was tested for reliability

using the Cronbach method and an index of 0.89 was established. A criterion mean of 2.50 was set to answer the research questions posed. Therefore, mean values 2.50 and above were considered high while any mean value less that 2.50 was considered low.

RESULTS

Presentation and Analysis of Data to Answer Research Questions

Research Question 1: *What is the level of students' awareness in the management of cyber counter-intelligence for students in universities in Rivers State?*

Table 1: Analysis of mean score ratings of students opinions on the level of students' awareness in the management of cyber counter-intelligence for students in universities in Rivers State?

	Awareness of cyber counter-intelligence for students in the management of secondary schools in rivers state	Female Students			Male Students			Grand Mean and Decisions	
		$\bar{X}_f$	SD	Decisions	$\bar{X}_m$	SD	Decisions	$\bar{X}_f\bar{X}_m$	Decisions
1	Students have adequate knowledge of the introduction of cyber counter-intelligence	2.30	1.060	Low Level	2.33	1.020	Low Level	2.32	Low Level
2	Students have a good understanding of cyber counter-intelligence services	2.51	.990	High Level	2.33	.818	Low Level	2.43	Low Level
3	Students' are proficient in the use of cyberspace	2.57	.956	High Level	2.67	.862	High Level	2.62	High Level
4	Trainings are available for students to enhance their awareness of cyber counter-intelligence	2.55	1.075	High Level	2.46	.931	Low Level	2.51	High Level
5	Students are encouraged to use the cyberspace	2.59	.932	High Level	2.48	.901	High Level	2.54	High Level
6	Students are familiar with the facilities and services of cyber counter-intelligence	2.53	.830	High Level	2.30	.937	Low Level	2.42	Low Level
	Aggregate mean							**2.47**	**Low** Level

From data in table 1 above, the calculated mean scores in items 3, 4 and 5 are higher than the criterion mean of 2.50. This indicates that students' have a good understanding of cyber counter-intelligence services ($\bar{x}$ = 2.62), also there are trainings available for students' to enhance their awareness of cyber counter-intelligence ($\bar{x}$ = 2.51), thereby encouraging students' in the use of cyberspace ($\bar{x}$ = 2.54).

The mean scores for items 2 and 6 from the female students' response are above the criterion mean of 2.50 but from the male students' response are below criterion mean of 2.50, taken the both aggregate, a mean of ($\bar{x}$ = 2.43) and ($\bar{x}$ = 2.42) was obtained which is less than the criterion mean of 2.50; it indicate that level of students' understanding of cyber counter-intelligence services are low also students' may not be very familiar with the facilities and services of cyber counter-intelligence and in item 1 both respondents agree that students' have adequate knowledge of the introduction of cyber counter-intelligence

Combining the aggregate mean both male and female response, obtained 2.47, responses from the male and female students', this connote that the level of awareness in the management of cyber counter-intelligence is low.

Research Question 2: *What is the level of adoption of penetration testing practices in the management of cyber counter-intelligence among students in universities in Rivers State?*

Table 2: Analysis of mean score ratings of respondents' opinions on the level of adoption of penetration testing practices adopted in the management of cyber counter-intelligence among students in universities in Rivers State

	Penetration Testing Practices Adopted In The Management Of Cyber Counter-Intelligence Among Students In Universities In Rivers State	Female Students			Male Students			Grand Mean And Decisions	
		$\bar{X}$	SD	Decisions	$\bar{X}$	SD	Decisions	$\bar{X}_f \bar{X}_m$	Decision
7.	Users have right to provide protection against foreign intelligence operations	2.61	.984	High Level	2.64	.844	High Level	2.62	High Level
8.	The cyber counter-intelligence is under utilized	2.94	.879	High Level	2.37	.868	Low Level	2.67	High Level
9.	There are software available for counter-intelligence	2.52	.990	High Level	2.42	.886	Low Level	2.48	Low Level
10.	Students possess skills to manipulate activities encountered in cyberspace	2.63	.962	High Level	2.26	.751	Low Level	2.46	Low Level
11.	There are provision for users to practice cyber counter-intelligence (that is to prevent, deter, defeat, or manipulate the adversary)	2.73	.964	High Level	2.19	.984	Low Level	2.48	Low Level
12.	There are actions taken to identify and counter adversary intrusions	2.67	.976	High Level	2.52	.919	High Level	2.60	High Level
13..	Scholars have quick and equal opportunity to information	3.00	2.034	High Level	2.74	.844	High Level	2.88	High Level
14.	There are maintaining access provided to improve pen test	2.76	.984	High Level	2.41	.954	Low Level	2.60	High Level
15.	Students 'usage of cyberspace is low	2.79	.915	High Level	2.56	1.101	High Level	2.68	High Level
16.	There are efforts to minimizing the threat landscape	2.64	.883	High Level	2.20	.850	Low Level	2.45	Low Level
17.	Reports are analysed overall personnel, network, and information security	2.70	.905	High Level	2.68	.883	High Level	2.69	High Level
18.	Users are provided with bypass of network to infiltrate the target	2.48	.990	Low Level	2.26	1.005	Low Level	2.38	Low Level
19.	Security evaluation is encouraged	2.64	.883	High Level	2.76	.815	High Level	2.69	High Level
20.	Performing regular vulnerability assessments internally or externally to counter cyber-attack	2.57	.741	High Level	2.41	.783	Low Level	2.50	High Level
21.	There are online forums to gather information about adversary intelligence collection operations (capabilities, victims, tactics)	2.97	.811	High Level	2.44	1.136	Low Level	2.74	High Level
	Aggregate mean							**2.59**	**High Level**

Data presented in table 2 show that items 7, 12, 13, 14, 15 and 19 have a positive reaction rate with weighted mean scores which are all greater than the criterion mean of 2.50. This implies that respondents agree that users have right to provide protection against foreign intelligence operations ($\bar{x}$ = 2.62), there are actions taken to identify and counter adversary intrusions ($\bar{x}$ = 2.60), scholars have quick and equal opportunity to information ($\bar{x}$ = 2.88), there are maintaining access provided to improve pen test ($\bar{x}$ =

2.60). Although, students' 'usage of cyberspace is low ($\bar{x}$ = 2.68) and security evaluations are encouraged ($\bar{x}$ = 2.69).

Responses from the female students on items 8, 16, 20, and 21 have a high mean score on the statements that cyber counter-intelligence is under-utilized ($\bar{x}$ = 2.96), there are efforts to minimizing the threat landscape ($\bar{x}$ = 2.64), performing regular vulnerability assessments internally or externally to counter cyber-attack ($\bar{x}$ = 2.57) and there are online forums to gather information about adversary intelligence collection operations (capabilities, victims, tactics) ($\bar{x}$ = 2.97) but the male students responses is of a contrary view with low mean scores respectively ($\bar{x}$ = 2.37), ($\bar{x}$ = 2.20), ($\bar{x}$ = 2.41) and ($\bar{x}$ = 2.44), in the overall these items have a high mean scores from grand mean decision.

Furthermore, in items 11 and 16, the responses from female students have high mean score on the statements that there are provision for users to practice cyber counter-intelligence (that is to prevent, deter, defeat, or manipulate the adversary) ($\bar{x}$ = 2.73) and there are efforts to minimizing the threat landscape ($\bar{x}$ = 2.64) also the male students responses is of a contrary view with low mean scores of ($\bar{x}$ = 2.19) and ($\bar{x}$ = 2.20) respectively in the average have a low mean scores.

Respondents' opinions in item 18 for both female and male students are all low disagree that users are provided with bypass of network to infiltrate the target. The analysis on this research questions gave an aggregate mean of ($\bar{x}$ = 2.59) for female and male students, this is also greater than the criterion mean of 2.50 and it implies that the respondents agree that there are penetration testing practices adopted in the management of cyber counter-intelligence among students'.

Research Question 3: *What is the extent to which the vulnerability assessment is adopted in the management of cyber counter-intelligence among students in the universities in Rivers State?*

Table 3: Analysis of mean score ratings of respondents' opinions on the extent to which the vulnerability assessment is adopted in the management of cyber counter-intelligence among students in the universities in Rivers State

	Vulnerability Assessment Is Adopted In The Management Of Cyber Counter-Intelligence Among Students In The Universities In Rivers State	**Female Students**			**Male Students**			**Grand Mean And Decisions**	
		$\bar{X}$	**SD**	**Decisions**	$\bar{X}$	**SD**	**Decisions**	$\bar{X}_f \bar{X}_m$	**Decision**
22.	There are effort to find weak systems	2.61	.906	High Extent	2.41	.829	High Extent l	2.52	High Level
23.	Vulnerability assessment are taught to students to enhance their cyberspace usage	2.55	.821	High Extent	2.33	.771	Low Extent	2.45	Low Level
24.	Most of the network and wireless facilities undergo assessment	2.64	1.012	High Extent	2.26	.799	Low Extent l	2.47	Low Level
25.	Software applications undergo scanning process periodically	2.73	.709	High Extent	2.48	.919	Low Extent l	2.62	High Extent
26.	There are development and implementation of vulnerability patch	2.39	.778	High Extent	2.36	.844	Low Extent l	2.38	Low Extent
27.	Host assessment procedures are adopted in schools	2.46	.892	High Extent	2.35	.999	High Extent	2.41	Low Extent
28.	There are demonstrations on the need of vulnerability analysis among students.	2.50	.792	High Extent	2.52	.740	High Extent l	2.51	High Extent
29.	Administrators are allowed to update operational or configure new changes to improve cyber counter-intelligence	2.59	.898	High Extent	2.48	.834	Low Extent l	2.54	High Extent
30.	There are vulnerability management in place to improve cyber counter-intelligence.	2.89	.996	High Extent	2.68	.925	High Extent	2.80	High Extent
	Aggregate mean							**2.52**	**High Extent**

From the data in table 3 items 22, 28 and 30 portray high mean scores. So it is clear that there are effort to find weak systems ($\bar{x}$ = 2.52), there are demonstrations on the need of vulnerability analysis among students ($\bar{x}$ = 2.51) and there are vulnerability management in place to improve cyber counter-intelligence ($\bar{x}$ = 2.80). However, male and female students responses on items 23, 24 and 26 are in disagreement that vulnerability assessment are taught to students to enhance their cyberspace usage ($\bar{x}$ = 2.45), most of the network and wireless facilities undergo through assessment ($\bar{x}$ = 2.47) and there are development and implementation of vulnerability patch ($\bar{x}$ = 2.38). But in items 25 and 29 are in agreement that software applications undergo scanning process periodically ($\bar{x}$ = 2.62) and administrators are allowed to update operational or configure new changes to improve cyber counter-intelligence ($\bar{x}$ = 2.54). The aggregate mean score of **2.52** depicts that extent to which vulnerability assessment is adopted in the management of cyber counter-intelligence among students are high.

Hypothesis 1: There is no significant difference between the mean ratings of male and female students on the level of their awareness in the management of cyber counter-intelligence in universities in Rivers State.

Table 4: z-test analysis of the difference between the mean ratings of male and female students on the level of their awareness in the management of cyber counter-intelligence in universities in Rivers State;

Variables	N	$\bar{X}$	SD	Df	Cal-z-Value	Critical z-value	Decision
male students	404	14.54	3.729	897	. .823	±1.96	HO1 Accepted
Female Students	495	14.56	3.685				

In table 4 there is the analysis of z-test difference between of male and female students on the extent of their awareness in the management of cyber counter-intelligence for students in universities in Rivers State. The result of the z-test shows that the calculated z-value of .823 is less than the critical of ±1.96 at the degree of freedom 897 with 0.05 significant level of confidence. The null hypothesis is therefore accepted; therefore there is no significant difference between the mean ratings of male and female students on the level of their awareness in the management of cyber counter-intelligence in universities in Rivers State.

Hypothesis 2: There is no significant difference between the mean ratings of male and female students on the level of adoption of penetration testing practices in the management of cyber counter-intelligence among students in universities in Rivers State.

Table 5: z-test analysis of the difference between the mean ratings of male and female students on the level of adoption of penetration testing practices in the management of cyber counter-intelligence in universities in Rivers State

Variables	N	$\bar{X}$	SD	Df	Cal-z-Value	Critical z-value	Decision
Male students	404	38.3589	8.41789	897	.704	±1.96	HO2 Accepted
Female Students	495	38.1919	8.28671				

From data in table 5 the result of the z-test shows that the calculated z-value of .704 is less than the critical value of ±1.96 at the degree of freedom 897 with 0.05 significant level of confidence. Consequently, the null hypothesis is accepted. Therefore, there is no significant difference between the

mean ratings of male and female students on the level of adoption of penetration testing practices in the management of cyber counter-intelligence in universities in Rivers State.

Hypothesis 3: There is no significant difference between the mean ratings of male and female students on the extent to which vulnerability assessment is adopted in the management of cyber counter-intelligence in the universities in Rivers State.

Table 6: z-test analysis of the difference between the mean ratings of male and female students on the extent to which vulnerability assessment is adopted in the management of cyber counter-intelligence in the universities in Rivers State.

Variables	N	$\bar{X}$	SD	Df	Cal-z-Value	Critical z-value	Decision
Male Students	404	21.8515	5.47067	897	.651	±1.96	HO3 Accep2ted
Female Students	495	21.9091	5.38233				

In table 6 the result of the z-test shows that the calculated z-value of .651 is less than the critical value of ±1.96 at the degree of freedom 897 with 0.05 significant level of confidence. The null hypothesis is thus accepted. Therefore there is no significant difference between the mean ratings of male and female students on the extent to which vulnerability assessment is adopted in the management of cyber counter-intelligence in the universities in Rivers State.

DISCUSSION OF FINDINGS

1. Students do not have a good understanding of cyber counter-intelligence and they are not proficient and familiar with the management of cyber counter-intelligence. However, there is great need for more awareness training should be introduced for students to enhance their interest management of cyber counter-intelligence because there management skill is not sufficient, although should be encouraged to be involved in the management of cyber counter-intelligence..
2. There is penetration testing practices adopted in the management of cyber counter-intelligence among student. Findings also reveal that there are efforts by students' to minimizing the threat landscape, because they are encouraged to practice pen test.
3. Vulnerability assessment is taught to students to enhance their cyberspace usage, argue that most the network and wireless facilities should undergo through assessment to improve their services. Data available however, indicate vulnerability assessment is a very important procedure in cyber counter-intelligence.

Level of awareness in the management of cyber counter-intelligence among students of universities in Rivers State

In the study a critical look at table 3 reveals that students' have a good understanding of cyber counter-intelligence services, there are trainings available for students' to enhance their awareness of cyber counter-intelligence , which will encouraging students' in the use of cyberspace. Respondents' opinions confirm that level of students' understanding of cyber counter-intelligence services are low also students' may not be very familiar with the facilities and services of cyber counter-intelligence. Statistical analysis shows that there is no difference between the opinion of female and male students on whether students have adequate knowledge of the introduction of e-library facilities cyber counter-intelligence.

This result explains that the awareness of cyber counter-intelligence in the universities is not encouraging, because students need to have adequate knowledge of cyber counter-intelligence services and the use of its facilities, so that their academic goals will be achieved. Overtime students spend so much time in the cyber space visiting both relevant and non-relevant site, thereby poses them to some cyber-attacks. The introduction of cyber counter-intelligence in universities will assist students look at for cyber-attacks.

Therefore, there is need for students to have adequate knowledge of CCI and its importance, which can also be achieved through training, which could be periodic to help improve the quality of usage of the cyber space and improve students understanding of cyber counter-intelligence.

The present result is in agreement with some past research findings, for instance our findings align with previous research, reinforcing the significance of understanding and addressing cyber threats within the university environment. Notably, Dodel and Mesch's (2019) study indicated that while awareness of the severity of cyber threats was generally average, users implementing antivirus precautions demonstrated a normative behavior. This emphasizes the importance of establishing and maintaining cybersecurity measures as a standard practice.

Building on this, Kritzinger (2017) recommended a heightened focus on cyber-safety awareness programs, emphasizing the existing gap in knowledge, which is notably absent from formal educational curricula. This highlights the urgent need for educational institutions to incorporate cyber safety into their programs and promote a culture of awareness among students and staff. Rezgui and Marks (2008) emphasized the imperative to initiate and foster information security awareness in the university environment. Their insights underscored that factors such as conscientiousness, cultural assumptions, and social conditions significantly influence the behavior and attitude of university staff. Moreover, their suggestion that awareness of cyber counter-intelligence should be actively encouraged aligns with our own observations and findings.

Supporting this perspective, Kam and Katerattanakul's (2014) research reinforced the need to promote information security practices in higher education. They highlighted the influential role of stakeholders in shaping normative expectations, thereby impacting regulative expectations. This underscores the importance of involving all relevant parties in the development and implementation of effective cybersecurity measures within academic institutions.

Furthermore, Abraham and Nwokoro's (2020) assertion that educators are yet to fully acknowledge and address the challenges associated with internet usage and the imperative for safety resonates with our own conclusions. It indicates a crucial area for improvement, emphasizing the necessity for educators to proactively engage with the evolving landscape of online threats and incorporate relevant safety measures into their teaching practices.

The graphical representation of our observations, as depicted in Figure 4.1 on page 186, serves as a visual testament to the prevailing situation. The majority of public universities examined in this study appear to lag in the adoption of cyber counter-intelligence practices. This underscores the urgency for these institutions to fortify their cybersecurity posture through increased awareness, comprehensive training, and the establishment of proactive measures to safeguard against cyber threats. Although, they all have virtual class room, in term of sitting capacity University of Port Harcourt has the highest sitting capacity for virtual classes, followed by Rivers State University and Ignatius Ajuru University of Education coming behind. Furthermore, the three public institutions considered in this works are fully involved in cyber space usage most especially, online registration and payment of fess, dues and many others, through the school website. Based on the synthesis of existing research and our own observations, several key recommendations emerge. Firstly, universities should prioritize the establishment of comprehensive cyber counter-intelligence training programs for both staff and students. These programs should not only focus on technical aspects but also on cultivating a culture of cybersecurity awareness.

Secondly, there is a pressing need for educational institutions to integrate cyber safety into formal curricula. By doing so, universities can ensure that students graduate with a foundational understanding of cybersecurity principles, preparing them for the digital challenges of the modern world.

Additionally, universities should actively involve stakeholders in the development and implementation of cybersecurity policies. This collaborative approach ensures that the diverse perspectives of administrators, faculty, students, and IT professionals are considered, fostering a more robust and effective cybersecurity framework. Furthermore, recognizing the influence of cultural assumptions and social conditions on staff behavior, universities should implement targeted awareness campaigns that address the specific challenges and concerns within their unique organizational context.

The test of hypothesis 1 in table 4 showed that there is no significant difference between the mean ratings of male and female students on the extent of their awareness in the management of cyber counter-intelligence for students in universities in Rivers State. Male and female students are of the same opinion on the level of their awareness in the management of cyber counter-intelligence in universities in Rivers State

Level of adoption of penetration testing practices in the management of cyber counter-intelligence among students in universities in Rivers State

The result in Table 4 indicate that users have right to provide protection against foreign intelligence operations, but cyber counter-intelligence is under-utilized, there are actions taken to identify and counter adversary intrusions, scholars have quick and equal opportunity to current information on CCI, there are maintaining access provided to improve pen test but students 'usage of cyberspace on CCI is low, although there web platform for security evaluation also there are report, online forums to gather information about adversary intelligence collection operations (capabilities, victims, tactics) and analysed overall personnel, network, and information security, to encourage regular vulnerability assessments internally or externally to counter cyber-attack. Responses' agree that cyber counter-intelligence is under-utilized; students are not provided with bypass of network to infiltrate the target on cyber space, there are efforts to minimizing the threat landscape, performing regular vulnerability assessments internally or externally to counter cyber-attack and there are online forums to gather information about adversary intelligence collection operations (capabilities, victims, tactics), but the male students responses is of a contrary view with low mean scores, in the overall it has a high mean response, showing that the penetration testing practices are useful tool to help enhance cyber counter-intelligence .

This result is in line with the findings of Sahri, *et al.*, (2014) which indicate that penetration testing process for web application in early stage is expected will reduce the chances of the web application being exploited as the internal penetration tester must check for any vulnerabilities found in the web application before it being deployed in the server. Therefore, the vulnerabilities found must be corrected and the re-check process has to be done so that only ZERO vulnerabilities and validated web application can be hosted in the university's server. The rapid development of digital infrastructures has provided cyber attackers with increasingly sophisticated toolkits, enabling them to infiltrate online systems and compromise vast troves of sensitive data. As the adage goes, prevention is better than cure. This paper explores the pivotal role of Penetration Testing (PT) in not only defending against illegal cyber-attacks but also proactively identifying potential vulnerabilities. By delving into the phases of data reduction, data analysis, and data classification, PT emerges as a powerful strategy for securing online systems and safeguarding sensitive information.

Kao *et al.* (2020) underscores the alarming rise in cybercrimes, highlighting the urgent need for robust cybersecurity measures. With the proliferation of sophisticated toolkits, cyber attackers can exploit vulnerabilities in online systems, posing a severe risk to the integrity and confidentiality of sensitive data. This escalation in cyber threats necessitates a proactive and comprehensive approach to cybersecurity. Penetration Testing (PT) stands out as a proactive and pre-emptive measure to counter cyber threats(Catalano et al., 2021; Al-Saraireh,2021; Masarweh & Al-Saraireh, 2022; Nguyen & Uehara 2023;Domínguez-Dorado et al.,2023; Yulianto et al., 2023; Yi & Liu 2023; Ghanem et al. & Krichen, 2023). Unlike traditional security approaches that focus solely on defence mechanisms, PT involves simulating real-world cyber-attacks to identify and rectify potential vulnerabilities. By adopting a preventive stance, organizations can fortify their defences and mitigate the risk of falling victim to malicious cyber activities. Penetration Testing comprises three integral phases: data reduction, data analysis, and data classification. These phases collectively form a structured approach to assessing and enhancing cybersecurity.

- Data Reduction: In this initial phase, the vast amount of collected data is distilled to extract relevant information. This process streamlines the focus of the penetration test, allowing for a more targeted and effective analysis of potential vulnerabilities.

- Data Analysis: The distilled data is subjected to thorough analysis, employing various testing techniques to simulate real-world cyber-attacks. This phase aims to uncover weaknesses in the system's defences, providing valuable insights for strengthening security measures.
- Data Classification: The final phase involves categorizing the identified vulnerabilities based on their severity and potential impact. This classification guides organizations in prioritizing their response, focusing on addressing the most critical threats first.

The efficacy of Penetration Testing extends beyond immediate threat mitigation. It serves as a proactive strategy for organizations to continuously improve their cybersecurity posture. By regularly conducting penetration tests, organizations can stay one step ahead of cyber adversaries, adapting and fortifying their defences in response to evolving threats. In conclusion, the escalating threat of cybercrimes demands a proactive and comprehensive approach to cybersecurity. Penetration Testing emerges as a crucial strategy, not only for defending against cyber-attacks but also for identifying and rectifying potential vulnerabilities. The structured phases of data reduction, data analysis, and data classification ensure a thorough examination of system weaknesses, allowing organizations to fortify their defenses and mitigate risks effectively. As information technology continues to advance, the integration of Penetration Testing into cybersecurity frameworks becomes paramount in safeguarding sensitive data and maintaining the integrity of online systems.

The hypothesis 2 in Table 5 was accepted because there is no significant difference between the mean ratings of male and female students on the extent of penetration testing practices adopted in the management of cyber counter-intelligence among students in universities in Rivers State. Male and female students are of the same opinion on the extent of penetration testing practices adopted in the management of cyber counter-intelligence in universities in Rivers State.

Extent to which the vulnerability assessment is adopted in the management of cyber counter-intelligence among students in the universities in Rivers State

Finding from the study in Table 5 shows that there are efforts to find weak systems, also there are demonstrations on the need of vulnerability analysis among students and there are vulnerability management in place to improve cyber counter-intelligence

Respondents' had negative views on the items which state that vulnerability assessment are taught to students to enhance their cyberspace usage, most of the network and wireless facilities undergo through assessment and there are development and implementation of vulnerability patch.

Male and female are in agreement that software applications undergo scanning process periodically also administrators are allowed to update operational or configure new changes to enhance vulnerability assessment and improve cyber counter-intelligence. The findings of Muniandy et al. (2017) are in agreement to the present study in terms of unsafe practices among undergraduate students in password usage, email management, and data backup processes. The identified discrepancy between perceived knowledge and vulnerability to cyber threats emphasizes the need for targeted interventions to enhance cybersecurity awareness and practices among the student population. Additionally, Maranga and Nelson's (2019) broader perspective underscores the overarching importance of computer security in higher education institutions, necessitating proactive measures to address the heightened interconnectivity of digital devices. Muniandy et al. (2017) delve into the prevalent unsafe practices among undergraduate students in password usage, email management, and data backup processes. Despite considering themselves knowledgeable users of cyberspace, a significant number of students remain susceptible to cyber-attacks. The paradox highlighted by Muniandy et al. (2017) reveals incongruence between students' claimed knowledge of cyberspace and their vulnerability to cyber threats, emphasizing the imperative for a closer examination of the gap between theoretical awareness and practical cybersecurity habits among the student population.

Maranga and Nelson's (2019) contextualization emphasizes the increasing significance of computer security in institutions of higher learning. The surge in cyberspace activities within educational settings

necessitates a comprehensive approach to safeguarding digital assets. The heightened interconnection of computer devices amplifies the urgency of addressing vulnerabilities to protect the integrity of academic and personal information. The interconnected nature of these devices underscores the need for institutions to implement robust cybersecurity policies.

Given the identified challenges, it is imperative to develop targeted strategies to bridge the gap between knowledge and practical cybersecurity habits among undergraduate students. Educational institutions should prioritize comprehensive cybersecurity awareness programs that specifically address issues related to password security, email management, and data backup processes. These programs should not only focus on theoretical knowledge but also impart practical skills, ensuring that students can effectively implement cybersecurity measures in their daily digital interactions. Moreover, Maranga and Nelson's (2019) emphasis on the interconnected nature of computer devices underscores the need for institutions to implement robust cybersecurity policies. This includes regular updates on security protocols, ensuring that both hardware and software are equipped to withstand evolving cyber threats. Collaborative efforts between educational institutions and cybersecurity experts can facilitate the development of tailored security measures that align with the unique challenges faced by students and academic staff.

To fortify cybersecurity defences, collaborative efforts between educational institutions and cybersecurity experts are crucial. Regular updates on security protocols for both hardware and software must be prioritized to withstand evolving cyber threats. Tailored security measures should be developed in collaboration with cybersecurity experts to address the unique challenges faced by students and academic staff. In conclusion, the multifaceted nature of cyber threats demands a holistic approach to cybersecurity in higher education institutions.

The insights from Muniandy et al. (2017) underscore the need for targeted interventions to bridge the gap between theoretical knowledge and practical cybersecurity habits among undergraduate students. Maranga and Nelson's (2019) broader contextualization emphasizes the urgency of implementing robust cybersecurity policies to safeguard interconnected digital devices. By prioritizing comprehensive cybersecurity awareness programs and engaging in collaborative security measures, educational institutions can fortify their defenses, empowering students and academic staff to navigate the digital landscape securely. However, Hypothesis 3 in table 6 was accepted which means that there is no significant difference between the mean ratings of male and female students on the level to vulnerability assessment is adopted in the management of cyber counter-intelligence among students in the universities in Rivers State. Both male and female students are of the same opinion on the extent to which vulnerability assessment is adopted in the management of cyber counter-intelligence in the universities in Rivers State.

CONCLUSION

In the ever-evolving landscape of cyberspace, the role of cyber counter-intelligence stands as a linchpin for promoting growth and ensuring the security of digital environments. This paper delves into the multifaceted aspects of managing cyber counter-intelligence in tertiary institutions, with a focus on its impact on students' academic pursuits. The discussion encompasses the various components of cyber counter-intelligence, emphasizing the need for up-to-date security measures and a proactive approach to meet the evolving needs of users. The management of cyber counter-intelligence plays a pivotal role in facilitating students' access to academic resources. By providing a secure and well-organized cyber space, students can navigate the digital realm without hindrance, ensuring seamless sourcing of materials for their academic needs. This not only streamlines the learning process but also fosters a conducive online environment that supports scholarly endeavours.

To ensure the efficacy of cyber counter-intelligence, a comprehensive approach is essential. This includes access to current security trail feeds, the deployment of email and database honeypots, penetration testing, and vulnerability assessments. The integration of these elements creates a robust defence mechanism, allowing information to be accessed without fear of compromise. It underscores the importance of staying abreast of emerging cyber threats and employing proactive measures to fortify digital security. The

benefits derived from managing cyber counter-intelligence in tertiary institutions are significant. Improved data security, streamlined access to information, and enhanced protection against cyber threats are among the key advantages. However, it is crucial to recognize that these benefits come with the responsibility of ensuring the sustainability and periodic upgrade of cyber counter-intelligence systems to meet the ever-evolving needs of users. As cyber counter-intelligence contributes to a secure online environment, there is a simultaneous need to guide and promote responsible use of cyberspace among students. Observations by researchers have indicated instances where students engage in non-academic activities, such as watching movies and irrelevant social interactions. Therefore, efforts to increase awareness among learners and researchers should be complemented by measures that steer the cyber space towards its intended purpose, fostering an environment conducive to academic exploration. Ensuring the effectiveness of cyber counter-intelligence goes beyond technical measures; it requires providing security and guidance for users. Establishing protocols and guidelines that restrict certain online activities aligns with the overarching goal of assisting students in remaining focused during their cyber space engagements.

By channelling users toward their academic objectives, institutions contribute to a purpose-driven and secure online learning environment. While acknowledging the current benefits of managing cyber counter-intelligence, it is imperative to emphasize the importance of sustainability and continuous upgradation. The dynamic nature of cyber threats demands a proactive approach, necessitating regular assessments, updates, and improvements to the cyber counter-intelligence framework. This iterative process ensures that institutions remain resilient in the face of emerging cyber challenges.

In conclusion, the pivotal role played by cyber counter-intelligence in fostering the growth and ensuring the security of cyberspace within tertiary institutions cannot be overstated. The profound positive impact on students' academic pursuits, which is facilitated by a well-managed cyber counter-intelligence system, serves as a testament to its significance in the contemporary educational landscape. The multifaceted benefits derived from this approach, spanning enhanced data security to the seamless access of academic resources, underscore the imperative of continuous efforts in managing and upgrading cyber counter-intelligence measures. As institutions increasingly prioritize raising awareness and guiding responsible use of cyberspace, it is essential to recognize the broader goal: the creation of a secure and purpose-driven digital environment. This encompasses not only securing sensitive data but also fostering an environment that encourages meaningful academic exploration. Tertiary institutions, therefore, need to proactively address these imperatives to ensure that cyber counter-intelligence remains not only a robust safeguard but also an enabler of academic innovation.

The ongoing evolution of cyber threats necessitates a dynamic and adaptive approach to cyber counter-intelligence. Institutions must continually assess and enhance their cybersecurity measures to stay ahead of potential risks. This involves investing in cutting-edge technologies, conducting regular training sessions for staff and students, and fostering a culture of cybersecurity awareness. Furthermore, collaboration within and beyond the academic community is paramount. Sharing best practices, insights, and threat intelligence can fortify the collective defence against cyber threats. Establishing partnerships with industry experts, governmental agencies, and other educational institutions can provide valuable resources and insights for bolstering cyber counter-intelligence capabilities.

In the ever-changing landscape of cyberspace, institutional leadership plays a crucial role. Leaders need to prioritize cybersecurity initiatives, allocate adequate resources, and champion a culture of cybersecurity awareness. This top-down commitment is instrumental in creating a resilient cybersecurity posture within tertiary institutions.

In summary, as we navigate the complexities of the digital age, the role of cyber counter-intelligence in securing and advancing the academic landscape is paramount. Tertiary institutions must embrace the challenges and opportunities presented by cyberspace, recognizing cyber counter-intelligence as a linchpin for safeguarding intellectual assets, fostering innovation, and ensuring the continued growth of academic excellence in the digital era. By taking proactive and collaborative measures, institutions can

fortify their cybersecurity defences, thereby creating a secure and conducive environment for academic pursuits in the 21st century.

RECOMMENDATIONS

1. The study also identified low level of awareness in the use of cyber counter intelligent also increase the level of attention to students during cyber space usage and less cyber security exposure.
2. Schools should provide free internet, to encourage student in engaging cyber counter intelligent also understand the state of art in the usage of cyber space.
3. Based on the results that training for students to enhance their interest in cyber counter-intelligence is not sufficient, there is need for students to have a better understanding of the modern technologies that are introduced to make cyber counter-intelligence services, effective and easy for researchers to use. Therefore, training and re-training should be introduced to enhance their knowledge and encourage the level of usage.
4. There should be efforts by students' to minimizing the threat landscape, because they are encouraged to practice pen test.
5. That students should be taught vulnerability assessment, to enhance their level of usage in the cyber space also argue that most of the network and wireless facilities should undergo through assessment to improve their services.

REFERENCES

Abraham, L. N., & Nwokoro, C. O. (2020). Achieving Cyber Safety in Junior Post-secondary Schools in Rivers State, Nigeria. The International Journal of Humanities & Social Studies. 8(4), 141–147.

Al-Saraireh, J. M. (2021). Enhancing the Penetration Testing Approach and Detecting Advanced Persistent Threat Using Machine Learning (Doctoral dissertation, Princess Sumaya University for Technology).

Andini, N. K. T., Damayanti, N. M. A. N. P., Sari, N. K. W. P., Fkun, E., & Erkamim, M. (2023). Cybercrime and Threats to the Electoral System. Journal of Digital Law and Policy, 3(1), 26-37.

Ashraf, A., König, C. J., Javed, M., & Mustafa, M. (2023). "Stalking is immoral but not illegal": Understanding Security, Cyber Crimes and Threats in Pakistan. In Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023) (pp. 37-56).

Baniulyte, G., Rogerson, N., & Bowden, J. (2023). Going paperless–Qualitative monitoring of staff morale during the transition from paper to electronic health records. Heliyon, 9(10).

Beierle, J., Algorri, M., Cortés, M., Cauchon, N. S., Lennard, A., Kirwan, J. P., Oghamian, S. & Abernathy, M. J. (2023). Structured content and data management—enhancing acceleration in drug development through efficiency in data exchange. AAPS open, 9(1), 11.

Catalano, C., Afrune, P., Angelelli, M., Maglio, G., Striani, F., & Tommasi, F. (2021). Security Testing Reuse Enhancing Active Cyber Defence in Public Administration. In ITASEC (pp. 120-132).

Dodel, M., & Mesch, G. (2019). An integrated model for assessing cyber-safety behaviors: How cognitive, socioeconomic and digital determinants affect diverse safety practices. Computers & Security, 86, 75–91. https://doi.org/10.1016/j.cose.2019.05.023

Domínguez-Dorado, M., Rodríguez-Pérez, F. J., Carmona-Murillo, J., Cortés-Polo, D., & Calle-Cancho, J. (2023). Boosting Holistic Cybersecurity Awareness with Outsourced Wide-Scope CyberSOC: A Generalization from a Spanish Public Organization Study. Information, 14(11), 586.

Federal Republic of Nigeria. (2004). National policy on education. NERDC.

Flemming, D., & Hübner, U. (2013). How to improve change of shift handovers and collaborative grounding and what role does the electronic patient record system play? Results of a systematic literature review. International journal of medical informatics, 82(7), 580-592.

Ghanem, M. C., Chen, T. M., & Nepomuceno, E. G. (2023). Hierarchical reinforcement learning for efficient and effective automated penetration testing of large networks. Journal of Intelligent Information Systems, 60(2), 281-303.

Jamshidi, M., Dehghaniyan Serej, A., Jamshidi, A., & Moztarzadeh, O. (2023). The meta-metaverse: ideation and future directions. Future Internet, 15(8), 252.

Kala, E. S. M. (2023). Critical Role of Cyber Security in Global Economy. Open Journal of Safety Science and Technology, 13(4), 231-248.

Kam, H.-J., & Katerattanakul, P. (2014). Information Security in Higher Education: A Neo-Institutional Perspective. Journal of Information Privacy and Security, 10(1), 28–43. https://doi.org/10.1080/15536548.2014.912482

Krichen, M. (2023). Formal Methods and Validation Techniques for Ensuring Automotive Systems Security. Information, 14(12), 666.

Kritzinger, E. (2017c). Growing a cyber-safety culture amongst school learners in South Africa through gaming. South African Computer Journal, 29(2). https://doi.org/10.18489/sacj.v29i2.471

Maranga, J., & Nelson, M. (2019). Emerging Issues in Cyber Security for Institutions of Higher Education. 8.

Masarweh, A., & Al-Saraireh, J. (2022). Threat led advanced persistent threat penetration test. International Journal of Security and Networks, 17(3), 203-219.

Muniandy, L., Muniandy, B., & Samsudin, Z. (2017). Cyber Security Behaviour among Higher Education Students in Malaysia. Journal of Information Assurance & Cybersecurity, 1–13. https://doi.org/10.5171/2017.800299.

Nguyen, H. V., & Uehara, T. (2023). Multilayer Action Representation based on MITRE ATT&CK for Automated Penetration Testing. Journal of Information Processing, 31, 562-577.

Nwokoro, C. O. (2016). Securing communication technologies for national development. The Proceedings of 2nd Computer Science Conference on Cyber Security and the Emerging African Economies, 2, 43–48.

Nwokoro, C. O. (2017). Teaching in a digital World: The role of e-learning facilities. In The teaching profession and teaching in a digital world (C. Williams, J. D. Asodike, V. N. Duru (Eds.), pp. 320–326). Pearl Publishers.Duvenage, P., Von Solms, S., & Corregedor, M. (2015). The Cyber Counter-intelligence Process—A Conceptual Overview and Theoretical Proposition. 13.

Riega-Virú, Y., Nilupu-Moreno, K., Salas-Riega, J. L., & Ninaquispe-Soto, M. (2023, December). Knowledge of cybersecurity against social cybercrime of female high school students. In 2023 IEEE 3rd International Conference on Advanced Learning Technologies on Education & Research (ICALTER) (pp. 1-4). IEEE.

Sahri, Z., Abd Aziz, M. E. S., Zolkefley, K. I., Sadjirin, R., & Raus, M. I. M. (2014). Implementing IT Security Penetration Testing in Higher Education Institute. Australian Journal of Basic and Applied Sciences.

Sarkar, G., & Shukla, S. K. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. Journal of Economic Criminology, 100034.

Singh, D. (2023). Emerging Trends in Cyber Crimes. Sustainable Business and IT, 39-45.

Yi, J., & Liu, X. (2023). Deep Reinforcement Learning for Intelligent Penetration Testing Path Design. Applied Sciences, 13(16), 9467.

Yulianto, S., Abdullah, R. R., & Soewito, B. (2023, August). Comprehensive Analysis and Remediation of Insecure Direct Object References (IDOR) Vulnerabilities in Android APIs. In 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs) (pp. 23-28). IEEE.