AJSTME, Volume. 9, Issue 6. 531-539, October, 2023. https://www.ajstme.com.ng
ISSN: 2251-0141 (Print), 2971-6233 (Online)

# Investigating Cyber Security Threats and Preventive Polices in Higher Institutions in Northeast Nigeria

**Mustapha Umar, Ismail Abdulkarim Adamu & Joshua Umaru**
Department of Computer Science,
Gombe State Polytechnic, Bajoga
**Corresponding author:** aaismail@gspb.edu.ng

## Abstract

This research work investigated cybersecurity challenges affecting higher institutions in Northeast Nigeria and the cybersecurity policy available in the higher institutions for combating cyberattacks. The descriptive survey research design was adopted for the study. A sample of 99 respondents from four institutions, Gombe State University, Gombe State Polytechnic, Bajoga, Federal College of Education (Tech), Potiskum and Federal Polytechnic, Bauchi were selected for the study. The instrument for data collection was validated by experts in Computer Science and Information and Communication Technology directorate of the selected institutions, and has an overall reliability of 0.89. Mean, standard deviation and charts were used as methods of data analysis. The result shows that cybersecurity is a challenge in the higher institutions in Northeast Nigeria and the most common cyber challenges faced by the higher institutions are bypassing of payment on students' portals, forged registry information, alteration of students' records in the department, alteration of semester results and impersonation. Also, higher institutions in Northeast Nigeria do not have cybersecurity mechanisms and policies implemented in the institutions. Lack of awareness campaigns and training of staff on cybersecurity-related challenges were found to be the major causes of cybercrime in the higher education institutions in Northeast Nigeria. It was furthermore found that higher institutions in Northeast Nigeria solve their cybersecurity challenges by using staff in the institutions and the services of experts from outside the institutions. The study recommended awareness campaigns on cybersecurity and training of staff on cybersecurity challenges to reduce the havoc of cyberattacks in the higher institutions in Northeast Nigeria.

**Keywords:** Cybersecurity, Cybercrime, Higher Education Institutions, Northeast Nigeria, Policies

## Introduction

As cybercrime activities continue to become a major threat across all types of business ventures and organizations, the higher education sector is also not left out as one of the victims of cyber-attacks. Cybercrime has a direct link with the university system such as the breach of examination software and the leak of students' records on the internet (Al-Ghalib, 2020). This crime also extends to public and private organizations like Japan's maritime strategy compromise via the theft of information on a university server (Ban, 2018). Universities and other higher learning institutions have become a major target for cybercriminals because they handle and manage large amounts of sensitive and valuable data (Rohan et al., 2023; Dioubate et al., 2023). The cyber threats in the academic institutions range from individuals seeking illegal financial benefits or individuals whose aim is to hijack, steal, access and damage sensitive data. The continuous rotation of staff, annual enrollment of new students and free flow of the workforce also contribute to the increase in cyber security challenges bedevilling higher institutions (Joachim & Wangen, 2021).

Furthermore, cybersecurity challenges are exacerbated in higher institutions due to collaboration and information sharing among researchers in the academia either internally or externally in the system, which is not common in other business sectors. The more the interconnectivity among higher institutions, cyber-attacks become in crescendo (Sharma, 2021; Bandara et al., 2014). With the undermining of traditional openness and sharing customs in academia by organized criminal groups like the Silent Librarian Campaign, cybercrime activities are now gradually gravitating towards the boardroom (Chapman, 2019). In

spite of the fact that thousands of research publications in the academia on cyber security have been published on the internet yet, higher education institutions (HEI) have not strengthened their cyber security policy to combat cyber-attack within the system rather it is left at the mercy of technicians to fix (Joachim & Wangen, 2021; Sharma, 2021).

With the continuously evolving nature of the cyber security threats landscape in information technology, identifying and mapping out the detrimental threats on organizations due to the new tactics and tools used for the attacks becomes difficult (Joachim & Wangen, 2021; Rohan et al. 2023). However, the need for higher institutions to develop cyber security architecture and policy that will guard the institutions thereby having experts that will monitor the dynamics of cyber threats within the system and provide training to staff in order to safeguard the system from cyber-attacks becomes imperative.

Therefore, this research work investigated the trends of cyber threats affecting higher education and the role of cyber security performance in academic institutions in Northeastern Nigeria to monitor the weaknesses of cyber security policies utilized. Additionally, the work investigates the harmful effect of cyber-attacks on higher institutions and suggests cyber security policy to be adopted in preventing cyber-related crimes in higher institutions.

**Statement of the Problem**

With cyber-attacks becoming a major concern in higher education ranging from breaches of examination software and leaked of students' records on the internet in Australia to Japan maritime strategy compromise via the theft of information on a university server, there is a need to take necessary measures in safeguarding the server of our higher institutions. These challenges are due to the continuous increase of collaboration and sharing of information and interconnectivity among higher educational institutions and the growing record of vital and sensitive information available. With all these concerns, thousands of publications have been published on cybersecurity challenges in academia, yet, higher education itself often leaves cyber security challenges at the mercy of technicians to fix.

Considering the above challenges mentioned, there is no policy suggested to protect the HEI from cyber threats and attacks. However, there is a need for higher institutions to develop and enhance internal cyber security policies that will protect the institutions from the widespread effect of cyber-attacks. However, this research carried out a survey of the trends of cyber threats affecting higher education in northeastern Nigeria states, and monitored the role of cyber security performance, weaknesses of cyber security policies utilized and provided solutions.

**Purpose of the Study**

The main purpose of this study is to investigate cybercrime threats and preventive policies in higher institutions in Northeast Nigeria. The specific objectives of the study are to determine the:

1. Cyber security threats bedevilling higher institutions in Northeastern Nigeria
2. Type of cyber-attacks experienced in Northeast Nigeria's higher institutions
3. Areas where higher education institutions are facing cyberattacks in Northeast Nigeria
4. Frequency with which higher education institutions in Northeast Nigeria review their cybersecurity policies
5. Ways in which higher education institutions in Northeast Nigeria solve their cyber security challenges
6. Policy issues in cyber security within higher education institutions in Northeast Nigeria

**Methodology**

This study adopted a descriptive survey research design to collect and analyse data on cybersecurity issues affecting higher education institutions in the Northeast Nigeria.

The work covers some selected higher institutions in the northeastern states of Nigeria including Gombe State University, Federal College of Education (Tech), Potiskum, Yobe State, Federal Polytechnic, Bauchi and Gombe State Polytechnic, Bajoga. Questionnaire was used to collect data from the selected institutions. The instrument was validated by computer science lecturers and ICT staff of the selected institutions. While the reliability of the instrument was tested using Cronbach's alpha which yielded a reliability index of 0.89. The researcher with the help of two research assistants collected the data by administering the instrument and collecting it on the sport. This was to ensure maximum return rate. The data collected was analysed using descriptive statistics of mean, standard deviation and charts. For the interpretation of the research result mean score equal or greater than 2.5 is accepted while mean score less than 2.5 is rejected. Also, percentage rating equal or greater

AJSTME, Volume. 9, Issue 6. 531-539, October, 2023. https://www.ajstme.com.ng
ISSN: 2251-0141 (Print), 2971-6233 (Online)

than 50% is accepted while percentage rating less than 50% is rejected.

## Results

The results of this study were presented based on the objectives of the study as follows:

### Determination of Cyber Security Threats Bedevilling Higher Institutions in North Eastern Nigeria

To determines if cyber security issues exist in tertiary institutions in the northeast Nigeria, the percentage rating of the respondents on the existence of cyber security threats within their institutions were computed and result presented in Figure 1.

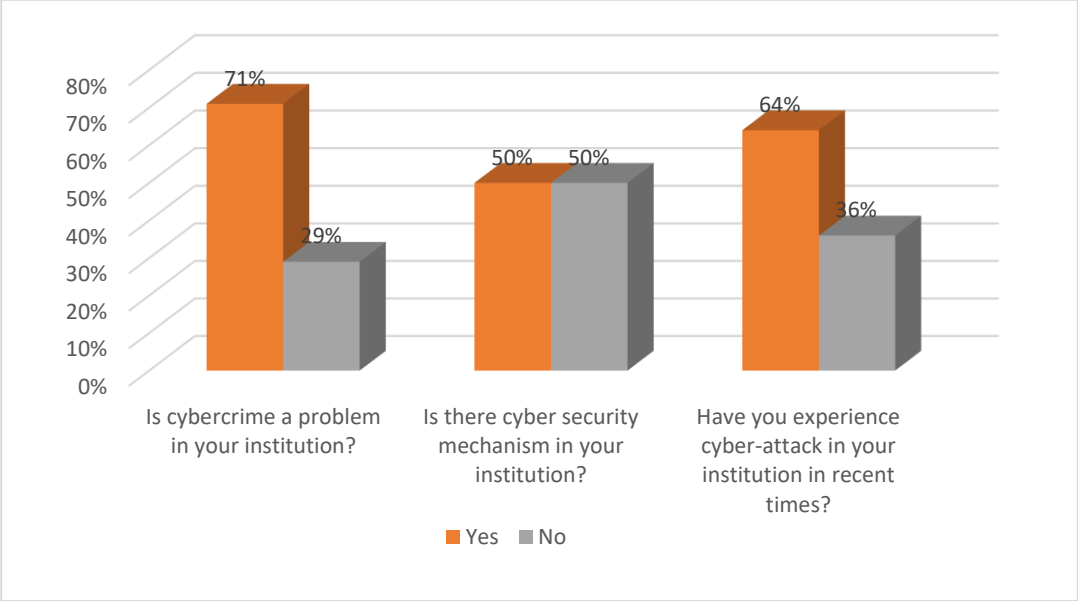


***Figure 1.*** *Percentage rating on Determination of Cyber Security Threats Bedeviling Higher Institutions in Northeastern Nigeria*

The results in Figure 1 show that the respondent agreed that cybercrime problems existed in their Institutions in Northeast Nigeria (71%). Also, 50% of the respondents indicated that there is no cybersecurity mechanism in the institutions to curb the cyber threats. Furthermore, 64% of the respondent agreed they have experienced cyberattack on their institutions in recent times. Therefore, cybercrime is a problem in Higher Education Institutions in the Northeast Nigeria, and most of the Higher Education Institutions in the region have experienced it. However, there is no cyber security mechanism to address that.

### Type of Cyber-Attacks Experienced in Northeast Nigeria Higher Institutions

The second objective of this study determined the type of cyber-attacks experienced in tertiary institutions in Northeast Nigeria. The mean and standard deviation of the respondents' response is presented in Table 1.

**Table 1. Mean and Standard Deviation of Types of Cyberattack Experienced in Northeast Nigeria Higher Institutions**

| S/N | Item Statement | N | $\bar{x}$ | SD | Remark |
|---|---|---|---|---|---|
| 1 | Credit card fraud | 98 | 3.57 | .556 | Agreed |
| 2 | Hacking and cracking | 98 | 3.40 | .513 | Agreed |
| 3 | Data diddling | 96 | 2.75 | .871 | Agreed |
| 4 | Cyber theft | 98 | 3.04 | .861 | Agreed |
| 5 | Forgery | 98 | 3.13 | .820 | Agreed |

**Key:** ***N*** *= Number of Respondents;* $\bar{x}$ *= Mean;* ***SD*** *= Standard Deviation,* $\bar{x} \geq 2.5$ *= Accepted;* $\bar{x} < 2.5$ *= Rejected*

Table 1 shows the mean and standard deviation of the types of cyberattacks experienced in Northeast Nigeria higher institutions. The results show that all the items are types of cyberattacks experienced in northeast

Nigeria higher institutions; credit card fraud had mean and SD ratings of (3.57±0.566), hacking and cracking had mean and SD ratings of (3.40±0.513), data diddling had mean and SD ratings of (2.75±0.871), cyber theft had mean and SD ratings of (3.04±0.861) and forgery had mean and SD ratings of (3.13±0.820). Therefore, the types of cyberattacks experienced in higher institutions in the northeastern Nigeria are: credit card theft, hacking and cracking, data diddling, cyber theft, and forgery.

**Areas where Higher Education Institutions are facing Cyberattacks in Northeast Nigeria**

To determine areas where the higher education institutions in Northeast Nigeria are experiencing cyber-attacks, the mean and standard deviation of the respondents' responses were computed and the result is presented in Table 2.

**Table 2. Mean and Standard Deviation of Areas where Higher Education Institutions are facing Cyberattack in Northeast**

| S/N | Item statement | N | $\bar{x}$ | SD | Remark |
|---|---|---|---|---|---|
| 1 | Bypassing payment on students' registration portal | 97 | 3.25 | .764 | Accepted |
| 2 | Forged registry information | 95 | 3.03 | .973 | Accepted |
| 3 | Alteration of semester result | 96 | 2.76 | .992 | Accepted |
| 4 | Alteration of student record in the department | 96 | 2.99 | .775 | Accepted |
| 5 | Impersonation | 96 | 3.18 | .562 | Accepted |

**Key: N** = *Number of Respondents;* $\bar{x}$ = *Mean;* ***SD*** = *Standard Deviation,* $\bar{x} \geq 2.5$ = *Accepted;* $\bar{x} < 2.5$ = *Rejected*

The results in Table 2 show that the respondents agreed to all the five items in this clusters as areas they face cyber-attacks since their mean ratings are all above the criterion mean of 2.50. They include: bypassing payment on student's registration portal (3.25±0.764), forgery of registry information (3.03±0.973), alteration of semester results (2.76±0.992), alteration of student's record in the department (2.99±0.775) and impersonation (3.18±0.562). Therefore, the areas in which higher institutions in Northeastern Nigeria are facing cybercrime related challenges are: bypassing payment on student's registration portal, forgery of registry information, alteration of semester results, alteration of student's record in the department, and impersonation.

**Frequency with which Higher Education Institutions in Northeast Nigeria Review their Cybersecurity Policies**

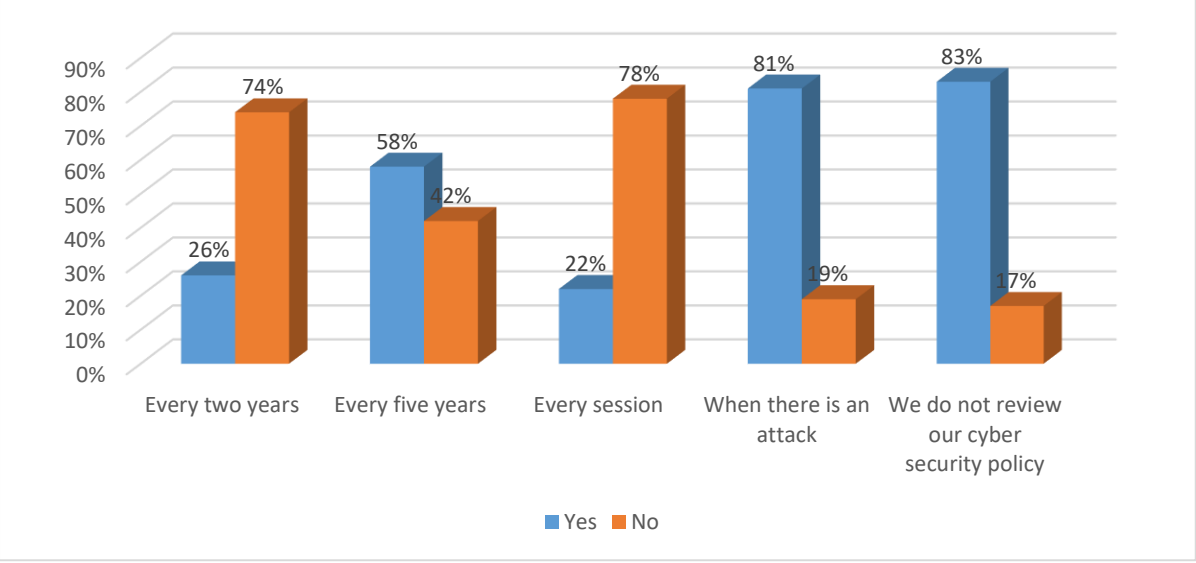


***Figure 2:*** *Percentage ratings on Frequency with which Higher Education Institutions in the Northeast Nigeria Review their Cybersecurity Policies)*

The result in Figure 2 shows that the respondent agreed with three items and disagree with two items. The items agreed upon by the respondents are: review of cybersecurity policy in their institution after five years (with a percentage rating of 58%), review of cybersecurity policy in their institution only when there is an attack (with a percentage rating of 81%) and institutions do not review their cybersecurity policy (with a percentage rating of 83%). The two items disagreed upon by the respondents are: review of cybersecurity policy after two years (with a percentage agreement rating of 26%) and review of cybersecurity policy every session (with a percentage agreement rating of 22%). Therefore, it could be said that the higher institutions in northeast Nigeria review it cybersecurity policy after five years, when there is an attack and, in some cases, do not even review it cybersecurity policy.

**Ways in Which Higher Education Institutions in the Northeast Nigeria Solve their Cyber Security Challenges**

Table 3. Mean and Standard Deviation of Ways in Which Higher Education Institutions in the Northeast Nigeria solve their Cyber Security Challenges

| S/N | Items Statement | N | $\bar{x}$ | SD | Remark |
|---|---|---|---|---|---|
| 1 | Using staff in the institution | 92 | 3.33 | .613 | Accepted |
| 2 | Employ the services of expert outside the institution | 91 | 3.37 | .852 | Accepted |

**Key: N** = *Number of Respondents;* $\bar{x}$ = *Mean;* ***SD*** = *Standard Deviation,* $\bar{x} \geq 2.5$ = *Accepted;* $\bar{x} < 2.5$ = *Rejected*

The result in Table 3 shows the way in which higher education institutions in Northeast Nigeria solve their cyber security challenges. Using staff within the institution to solve their cybersecurity challenges had a mean rating of (3.33±0.613), employing the services of experts outside the institution (3.37±0.852). Therefore, the ways in which higher education institutions in Northeast Nigeria solves their cyber security challenges are: using staff within the institutions, and employing the services of expert outside their institutions.

AJSTME, Volume. 9, Issue 6. 531-539, October, 2023. https://www.ajstme.com.ng
ISSN: 2251-0141 (Print), 2971-6233 (Online)

**5.6 Policy Issues in Cyber Security within Higher Education Institutions in Northeast Nigeria**

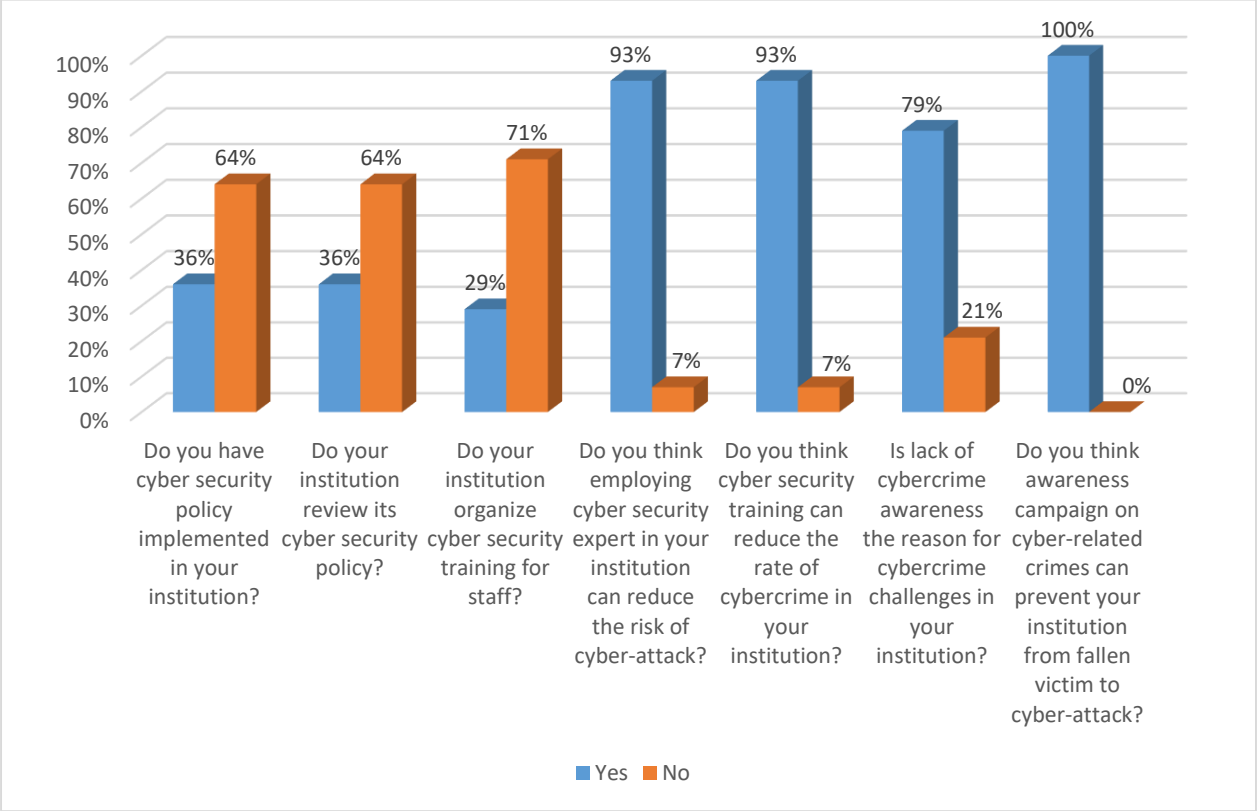


**Figure 3**: *Percentage ratings of Policy Issues in Cyber Security within Higher Education Institutions in Northeast Nigeria*

Result in Figure 3 shows that the respondents disagreed with three items and agreed to four items concerning cyber securities policies in their institutions. The disagreed items are: cyber security policy implementation in their higher institution (with an agreement rating of 36%), review of cybersecurity policy (with an agreement rating of 36%) and organization of cybersecurity training for staff (with an agreement rating of 29%). Furthermore, the respondents agreed that employing cybersecurity expert, and cybersecurity training in their institutions can reduce the rate of cybercrime (93% each). Also, it was agreed that lack of cybersecurity awareness is a major cause for cybercrime challenges in their institutions (79%). Finally, 100% of the respondents agreed that awareness campaign on cyber-related crimes can prevent their institution from falling victim to cyber-attack. Therefore, it could be said that there are no cyber security policies implemented, no review of cyber security policies, and an absence of training for staff on cybersecurity. However, employing cyber security experts in the institutions can reduce the risk of cyber-attacks, and cyber security training can reduce the rate of cybercrime. Furthermore, lack of cybercrime awareness is a reason for cybercrime challenges in the institutions. Awareness campaigns on cyber related crimes can prevent institution from fallen victim of cyber-attack.

**Discussion of Results and findings**

The results of this research work were discussed based on the objectives of the study:

**Determination of Cyber Security Threats Bedevilling Higher Institutions in Northeastern Nigeria**

The findings discovered that cybercrime is a problem in Higher Education Institutions in the Northeast Nigeria, and most of the Higher Education Institutions in the region have experienced it. However, there is no cyber security mechanism to address that. Cybersecurity is indeed a serious threat in Nigeria higher institutions most especially in the northeast. Bukhari and Samuel (2021) assert that in spite of the cybersecurity challenges in Nigeria universities, the institutions lack mechanisms installed in the institutions to combat these challenges. This is possible because higher institutions in Nigeria do not have budget for cybersecurity related

challenges that will help to develop standard framework for combating the cyber related crimes.

**Type of Cyber-Attacks Experienced in Northeast Nigeria Higher Institutions**

The result findings reveal that higher institutions in northeast Nigeria are experiencing credit card theft, hacking and cracking, data diddling, cyber theft, and forgery related cybercrime. According to Ankita (2021) higher institutions are faced with payment card fraud involving credit card not carriedout using hacking tool, unitended disclosure of sentitve information on website which becomes publicly available, hacking and malware involving illegal electronic entry by unathorized party or data loss by spyware and the lost of data due stolen of stationary electronic devices. This finding by ankita is discovered to be true from the findings in this research considering the nature of cyberattack experienced by higher institutions in northeastern Nigeria collated from the correspondent. This is possible because most higher institutions are automating their registration and payment processes online which may lead to credit card fraud and the exposure of sensitive data to unauthorized users online.

**Areas where Higher Education Institutions are facing Cyberattack in Northeast**

The result finding shows that the areas in which higher institutions in northeastern Nigeria are facing cybercrime related challenges are: bypassing payment on student's registration portal, forgery of registry information, alteration of semester results, alteration of student's record in the department, and impersonation. This is so because of individuals seeking illegal financial benefits or those whose aim is to hijack, steal, access and damage sensitive data. The continuous rotation of staff, annual enrolment of new students and free flow of the workforce also contribute to the increase in cyber security challenges bedevilling higher institutions (Joachim & Wangen, 2021). With the automation of student registration and payment of tuition fee by higher institutions online, it is possible for hackers to bypass the portal and perform illegal registration when the school portal is not secured. Also, student record can be altered and result manipulated due to insecure student portal.

**Frequency with which Higher Education Institutions in the Northeast Nigeria Review their Cybersecurity Policies**

The research findings show that higher institutions in northeast Nigeria review it cybersecurity policy after five years, when there is an attack and, in some cases, do not even review the cybersecurity policy. These assertions are true because the challenges for higher education institutions is the successful implementation of a cybersecurity strategy based on risk assessment. When cybersecurity violations occur at universities, it has been observed that regulations are less likely to be followed because security policy papers are not robustly implemented as observed in Malaysia by (Balla et al., 2023). This is possible because no cybersecurity policy papers are implemented in most higher institutions in northeast Nigeria which make it difficult for the institutions to know the areas of its cybersecurity weaknesses and provide solution when there is a cyberattack.

**Ways in Which Higher Education Institutions in the Northeast Nigeria Solve their Cyber Security Challenges**

Research findings shows that the ways in which higher education institutions in the Northeast Nigeria solves their cyber security challenges are: using staff within the institutions, and employing the services of expert outside their institutions. The problem with higher institutions is living their security challenges for an outsider to fix (Sharma, 2021; Joachim & Wangen, 2021). This is possible when the institution does not a cybersecurity expert to fix it cybersecurity challenges. However, this is a dangerous idea which may lead to some secret information of the institution being exposed to intruders. It will be good for Higher institutions to employ the services of cybersecurity expert within its institutions to solve its cybersecurity challenges to avoid their sensitive information been exposed to intruders.

**Policy Issues in Cyber Security within Higher Education Institutions in Northeast Nigeria**

The research finding shows that there are no cyber security policies implemented, no review of cyber security policies, and absence of training for staff on cybersecurity in higher institutions in northeast Nigeria. However, cyber security experts from the institutions can reduce the risk of cyber-attacks, and cyber security training can reduce the rate of cybercrime. Furthermore, lack of cybercrime awareness is a reason for cybercrime

challenges in the institutions. Awareness campaigns on cyber-related crimes can prevent higher institution from falling victim to cyber-attacks. According to Njoku et al. (2019) institutions in Nigeria do not have cybersecurity mechanism implemented which become a loophole for cybercrime. This is true because there is no funding available in higher institutions in Nigeria for combating cybercrime and providing cybercrime training and awareness to staff of the institutions. These makes the staff not to be familiar with the trends of cyber threats as a result, becomes victims of cyberattack.

## Conclusion

Cybersecurity is a challenge in higher institutions in recent times due to nature of sensitive data available. In this work, cyberthreat bedevilling higher institutions and polices available for mitigating these threats were investigated. The result shows that higher institutions in north east are facing cyberattack. The types of cybercrime faced by these institutions includes credit card fraud, hacking and cracking, data diddling, cyber theft, and forgery. The study shows the areas these attacks are perpetrated on higher institutions in northeast Nigeria includes bypassing of student's payment on registration portal, forged registry information, alteration of semester results, alteration of students' records in the department and impersonation. With all these challenges, the research discovered that institutions in northeast only review their cybersecurity policy after five years, when there is an attack, and in some cases don't even review the cybersecurity policy. The study further reveals that cybersecurity problems in higher institutions in northeast Nigeria is solved using staff in the institutions and services of expert outside the institutions. The study also shows that, institutions in Northeast do not have cybersecurity policy, do not review it cybersecurity policy and do not organize cyber security training for staff of the institutions. The research also identifies that lack of cybersecurity awareness campaign in higher institutions in northeast are contributing to cybercrimes challenges in these institutions. Finally, it is discovered that employing cybersecurity experts, training staff and creating awareness campaigns on cybersecurity can reduced the trends of cybersecurity challenges in higher institutions in Northeast Nigeria.

## Recommendations

Considering the findings in this research work, it was recommended that:

1. Higher institutions in the Northeast Nigeria should implement cybersecurity policy that will be reviewed every session.
2. Organise cybersecurity awareness and training to staff regularly and employ cybersecurity expert within the institution in order to combat cyber threats and attacks threatening the operation of higher institutions in the Northeast Nigeria.
3. The entire institutions in the northeast should be investigated to monitor the security challenges affecting these institutions.

## Acknowledgement

I sincerely want to appreciate Tertiary Education Trust Fund (Tetfund) for supporting and sponsoring this research work.

## Reference

Al-Ghalib, E. (2020, August 7). Australian universiies investigating 'deeply concerning' hack of controversial exam software . Australia

Andreea, B. (2015). Cyber-Attacks-Trends, Pattern and Security Countermeasures. *7th International Conference on Financial Criminology* (pp. 24-31). United Kingdom: Science direct.

Ankita, s. (2021). Review on Major Cyber security Issues in Educational Sector. *International Journal of Computer Sciences and Engineering, 9*(12), 26-29.

Balla, M. D., Wan, D. W., Zainol, F. A., & Salleh, F. (2023). The Role of Cybersecurity on the Performance of Malaysian Higher Education Institutions. *Jurnal Pengurusan, 67*, 1-12.

Ban, M. (2018, September 18). Universities the weak link when hackers strike Japan. Asia.

Bandara, I., Ioras, F., & Mahe, K. (2014). Cyber Security Concerns In E-Learning Education. *Proceedings of ICERI2014 Conference*, (pp. 0728-0734). Spain.

Bukhari, B., & Samuel, C. A. (2021). International Journal of Computer Sciences and Engineering. *Proceedings of the 1st Virtual Conference on Implications of Information and Digital Technologies for Development*, (pp. 853-866).

Chapman, J. (2019, April). How safe is your data? Cyber-security in higher education. *HEPIPolicy Note 12*, pp. 1-6.

Dian, D., & Mary, I. (2021). The Implementation of the Cybercrime Prevention Policy at The Metro Jaya Police Station in Central Jakarta.

*Proceeding of the 1st International Conference on Science and Technology in Administration and Management Information*, (pp. 1-13). Jakarta.

Dioubate, B. M., Norhayate, W. D., Anwar, Z. F., Fauzilah, S., Faiz, H. M., & Hai, L. O. (2023). The Role of Cybersecurity on the Performance of Malaysian Higher Education Institutions. *Journal Pengurusan* , 1-12.

Joachim, B. U., & Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet, 13*(39), 1-40.

Njoku, D.O., Nwokorie, E.C., Okolie, S.A., & Odii, J.N. (2019). Cyberspace Activities Awareness And Security Strategies In Tertiary Institutions In Nigeria. *Iconic Research And Engineering Journals, 3*(2), 439-445.

Obotivere, B. A., & Nwaezeigwe, A. O. (2020). Cyber Security Threats on the Internet and Possible Solution. *International Journal of Advanced Research in Computer and Communication Engineering, 9*(9), 92-97.

Prajna, D. I., Anas, S., Fabian, S. N., & Moch, F. R. (2023). The Reliability Analysis for Information Security Metrics in Academic Environment . *International Journal On Informatics Visualization*, 92-97.

Rohan, R., Funilkul, S., Chutimasku, W., Kanthmanon, P., Papasratorn, B., & Pal, D. (2023). Information Security Awareness in Higher Education Institutes: A Work in Progress. *15th International Conference on Knowledge and Smart Technology* (pp. 1-6). IEEE.

Samira, I., Daniel, I. N., & Ojeifoh, O. (2021). Types of Cybercrime and Approaches to Detection. *IOSR Journal of Computer Engineering, 23*(5), 24-26.

Sharma, A. (2021). Review on Major Cyber security Issues in Educational Sector. *International Journal of Computer Sciences and Engineering, 9*(12), 26-29.

Shivani, G., Akshada, P., & Rashmi, L. (2020). Importance of Cyber Security. *International Journal of Engineering Research and Technology, 8*(5), 1-3.

Stephen, K. (2023). Exploring public Cybercrime Prevention Campaigns and Victimization of Business: A Bayesian Model Averaging Approach. *Computers & Security*, 1-14.

Vadza, K. C. (2013). Cyber Crime & its Categories. *Indian Journal of Applied Research, 3*(5), 130-133.