International Journal of Natural & Applied Science
Volume 5, Number 3, September 2024
http://www.cedtechjournals.org
ISSN: 2756-4606

THE ROLE OF CYBER SECURITY POLICIES IN PROMOTING SAFE ONLINE BEHAVIOUR AMONG STUDENTS OF NIGERIAN TERTIARY INSTITUTIONS: A NORTH-EASTERN STATES PERSPECTIVE.

Abubakar Salisu[1]; **Anas Yunusa Adamu** [2] **and Bashir Tirmizi Yusuf** [3]
Computer Science Department,
Federal Polytechnic Bali, Taraba State
Email: sadiqsalisumar@gmail.com, yunusa.anas.ay@gmail.com,
bashirtirmiziyusuf@gmail.com

ABSTRACT

This study assessed the impact of cybersecurity policies on students' online behavior in tertiary institutions in northeastern Nigeria. Descriptive and Inferential statistics approach was employed, utilizing both surveys and interviews with a sample of 400 students. The research aimed to investigate the relationship between policy implementation and safe online practices among these students. The results indicated a statistically significant positive influence of cybersecurity policies on students' online activities, with key performance indicators showing improved online safety behavior. However, the study also identified several challenges that hinder full compliance with these policies. It is recommended that policies be enhanced, and targeted training programs introduced, to increase overall adherence and foster greater cybersecurity awareness and safety.

Keywords: *Cybersecurity Policies, Online Behavior, Tertiary Institutions, Online Safety, Compliance.*

INTRODUCTION

The rapid expansion of the internet has transformed how individuals, institutions, and businesses connect and operate globally. This connectivity has made it imperative to regulate human behavior online to ensure security and privacy. Inappropriate online behavior defined as actions that compromise digital safety, such as interacting with phishing links, downloading malware, or using infected storage devices poses a major challenge to cybersecurity. (Gratian, 2018). Students in tertiary institutions, particularly in northeastern Nigeria, represent a demography that frequently engages with the internet due to their academic and social activities. Their explorative nature makes them susceptible to both positive and negative online behavior. This vulnerability raises questions about the effectiveness of cybersecurity policies in shaping their online practices. While some research suggests that students in higher institutions are more prone to risky online behaviors, others highlight the potential for positive outcomes when security measures are in place (Ogutcu, 2021).

Nigeria as a country faces multiple threats on the cyberspace with the banking and financial sector taking the center stage. Failure to tackle these threats threatens to derail Nigeria's achievement of prosperity and security especially its information infrastructure, protection and resilience. Thus, to ensure cyberspace security Nigeria created the national cybersecurity policy in 2014 and the Nigerian cybercrime act 2015 (Adewunmi, 2021).

Despite the growing number of internet users in Nigeria, including students, there appears to be a lack of robust enforcement and adherence to cybersecurity policies. National efforts to regulate online behavior often fall short of addressing the complexities of modern cyber threats. For students, this disconnect between policy and practice means they are left more exposed to risks in cyberspace. The absence of clearly defined national and institutional cybersecurity policies further complicates efforts to promote online safety among this population. This study seeks to assess the extent to which these policies affect student behavior, examine how policies can promote safer online practices and identify the factors that hinder full compliance with these policies. Understanding these dynamics is essential for developing targeted interventions and strengthening cybersecurity awareness and adherence in educational institutions.

By addressing these objectives, this study will contribute to efforts aimed at improving cybersecurity practices among students, ensuring that both national and institutional policies are not only in place but effectively implemented and adhered to. Ultimately, the findings will serve to bridge the gap between policy creation and actual behavioral change, offering recommendations for enhancing the safety and resilience of students in the digital space.

RESEARCH QUESTIONS

The following research questions were formulated to explore the impact of cybersecurity policies on the online behavior of students in tertiary institutions in northeastern Nigeria:

1. To what extent do cybersecurity policies affect the online behavior of students in tertiary institutions in northeastern Nigeria?

2. How do cybersecurity policies influence the promotion of safe online practices among students in these institutions?

HYPOTHESES

This study investigates the impact of cybersecurity policies on students' online behavior in tertiary institutions located in northeastern Nigeria. The hypotheses below are formulated to guide the study in determining the relationship between policy implementation and online behavior:

i. **Ho1**: Cybersecurity policy does not significantly affect the online behavior of students in tertiary institutions in northeastern Nigeria.
ii. **Ho2**: Cybersecurity policy does not have a significant impact on ensuring safe online behavior among students in tertiary institutions in northeastern Nigeria.

LITERATURE REVIEW

The literature review examines existing research on cybersecurity policies, their definitions, and their significant role in shaping students' online behavior. It highlights the necessity of these policies in educational settings, especially given the increasing prevalence of cyber threats.

THE CONCEPT OF CYBERSECURITY POLICIES

Cybersecurity policies consist of a set of guidelines and rules developed by organizations and institutions to protect their information systems and networks from cyber threats and attacks. These policies define the organization's approach to cybersecurity, establish expectations for individual behavior, and outline procedures for responding to security incidents (Siyam & Hussain, 2021). Cybersecurity policies can cover a wide range of topics, including access control, password management, data protection, network security, incident response, and employee training. They can be tailored to address specific security risks and compliance requirements or provide a comprehensive framework for managing cybersecurity risks (Bulger et al., 2017). In the context of promoting safe online behavior among students, cybersecurity policies for educational institutions should address critical issues such as social media use, online bullying and harassment, appropriate use of technological resources, and responsible data sharing. For these policies to be effective, they must be communicated clearly to students, faculty, and staff, and enforced consistently, ensuring that students understand the importance of cybersecurity and are held accountable for their online actions (Abd Rahman et al., 2014).

The Role of Cybersecurity Policies on Students' Online Behavior

Research indicates that implementing cybersecurity policies in educational settings significantly impacts students' online behavior. For instance, Rieger et al. (2018) found that schools with established cybersecurity policies increased students' awareness of cyber risks, helping them develop safer online practices. Their study demonstrated that students who received cybersecurity training and understood relevant policies were less likely to engage in risky online behaviors. Similarly, Balci et al. (2019) reported that awareness of cybersecurity policies led students to exhibit more responsible online behavior. The research indicated that students who understood the implications of these policies were more inclined to report incidents of cyberbullying and avoid engaging in hazardous online activities. Similarly, Gao et al. (2019) emphasized that educational institutions implementing cybersecurity policies alongside training programs effectively reduced cybersecurity risks and fostered safe online behavior.

Nigeria had acquired a notoriety in criminal activities on the cyberspace especially financial scams using the internet. Most of the time, students and graduates taking a center stage in those crimes. It is argued that the problem arose as a result of direct consequences of the lapses in the enactment and implementation of cybersecurity policies (Roseline, 2021).

THEORETICAL LITERATURE REVIEW

This section explores the theoretical frameworks that underlie the understanding of cyber incidents and student behaviors in the context of cybersecurity policies. One prominent framework is the Social Norms Theory, which posits that individuals' perceptions of how others in their social group behave significantly influence their actions. Misperceived social norms can lead to behaviors that unnecessarily expose individuals to ridicule or harm. (Acosta et al., 2019). The Social Presence Theory also contributes to this discourse, focusing on how individuals form relationships during communication. It suggests that the low levels of social presence in online interactions—coupled with the anonymity afforded by the internet—can lead to uninhibited behavior among cyber aggressors. Consequently, individuals may act in ways online that they would not in face-to-face interactions, fostering an environment that is more impersonal and hostile (Tu, 2010; Joinson, 2011; Shariff & Hoff, 2007).

This review of the theories emphasizes the necessity of addressing these dynamics within cybersecurity policies aimed at educating students about safe online practices. The current study will employ Social Norms Theory as a foundational framework, adapting it to fit the specific context of northeastern Nigeria's educational institutions.

EMPIRICAL LITERATURE REVIEW

The empirical literature highlights various aspects of cyber incidents and the education surrounding them, particularly in relation to students. A cyber incident is defined as any illegal conduct perpetrated by individuals using electronic or digital means. While schools are making efforts to educate students about cyber incidents through various materials (Hills, 2017), these initiatives often occur in a manner detached from the environments where these incidents typically take place (Bulger et al., 2017). The effectiveness of educational programs can be limited when they do not address real-time occurrences in relevant contexts. Mhlanga (2021) argues that current initiatives predominantly operate offline, failing to provide practical solutions and recommendations for mitigating cyber incidents in real-life situations. Furthermore, there is insufficient emphasis on technical solutions within social networks that could remind students of behavioral norms, which might prevent the dissemination of harmful comments (Abd Rahman et al., 2014; Mhlanga, 2021b).

Research indicates that while awareness of internet usage is growing among students, their understanding of safe practices when engaging with information and communication technologies (ICTs) remains inadequate (Kritzinger, 2016). Students often receive mixed messages about online behavior as they strive for digital literacy, leading to gaps in the necessary support (Kritzinger, 2016). In Nigeria internet fraud in tertiary institutions are most of the time socially organized and highly networked. Cybercrime was reported to benefit in their schooling expenses and acquiring of properties such as cars. Integration of cybersecurity policies and check of unbridled corruption will go a long way ridding tertiary institution of such crimes (Oludayo and Ibrahim, 2022).

While Nigeria is developing its cybersecurity strategy. The country still needs to put some global best cybersecurity practices and policies into reality. Improved national cyber governance and accompanying internet propects would help Nigeria more appealing key player in the cyber security and job creation (Olalekan, 2023).

METHODOLOGY

This section outlines the research design, population, sampling techniques, sources of data, and data analysis methods employed in the study.

RESEARCH DESIGN

The study employed descriptive statistics research design, integrating both quantitative and qualitative approaches. This design allows for a comprehensive understanding of the impact of cybersecurity policies on students' online behavior by combining numerical data from surveys with qualitative insights from open-ended responses.

POPULATION OF THE STUDY

The target population for this study comprises all students enrolled in tertiary institutions across the northeastern region of Nigeria. This includes universities, polytechnics, and colleges of education within the six states of the region. Adamawa, Bauchi, Borno, Gombe, Taraba, and Yobe. The total population of students in these institutions is estimated at over 200,000 providing a diverse representation of various fields of study and academic levels.

SAMPLING TECHNIQUE AND SAMPLE SIZE

A stratified random sampling technique was employed to ensure that the sample adequately represents the various strata of the population based on state and institution type. The sample size of 400 participants was determined using the Cochran formula for sample size calculation:

$$n = \frac{Z^2 . P(1-P)}{e^2}$$

Where:

n = sample size

Z = Z-value (1.96 for 95% confidence level)

p = estimated proportion of the population (0.5 for maximum variability)

e = margin of error (0.05)

Substituting the values, we get:

$$n = \frac{(1.96)^2 . 0.5(1-0.5)}{0.05^2} = 384$$

To account for potential non-responses and ensure a more robust sample, the sample size was increased to 400 participants.

SOURCES OF DATA

Primary data were collected through the use of structured questionnaires designed to elicit responses related to students' online behavior and their awareness of cybersecurity policies. The questionnaire consisted of both closed-ended and open-ended questions, allowing for quantitative analysis and qualitative insights.

TECHNIQUES OF DATA ANALYSIS

The data collected were analyzed using both descriptive and inferential statistical techniques. Descriptive statistics were used to summarize the demographic characteristics of the participants, while inferential statistics, specifically the Chi-square (χ^2) test, were employed to test the hypotheses. The Chi-square formula is represented as follows:

$$\chi^2 = \sum \frac{(F_O - F_E)}{F_E}$$

Where:

- F_O = frequency observed
- F_E = frequency expected

The null hypothesis (H_0) will be rejected if the calculated χ^2 value exceeds the tabulated χ^2value at the specified degrees of freedom and significance level.

In addition, qualitative data obtained from open-ended questions will be analyzed thematically to identify common patterns and insights related to students' experiences and perceptions of cybersecurity policies.

DATA PRESENTATION, ANALYSIS, AND INTERPRETATION

This section outlines the procedure followed to test the formulated hypotheses using statistical software. Specifically, the Chi-square test was employed to assess the relationship between cybersecurity policies and students' online behavior. The analysis was conducted using the Statistical Package for the Social Sciences (SPSS), a widely used software for statistical analysis.

TEST OF HYPOTHESES

This study formulated two null hypotheses to guide the analysis. Each hypothesis was tested using data gathered from the survey responses. The Chi-square test was used to assess the relationship between cybersecurity policies and students' online behavior. The analysis was carried out using statistical software to ensure accuracy and transparency in the computation process.

Test of Hypothesis One

Ho1: Cybersecurity policies do not affect students' online behavior in northeastern Nigeria.

Questionnaire Overview

The survey consisted of multiple questions aimed at understanding how cybersecurity policies influence students' online behavior. For this hypothesis, questions A1, A2, A3, and A4 represent different aspects of students' perceptions regarding cybersecurity policies and their impact on online behavior. The questions are as follows:

A1: Do you believe cybersecurity policies in your institution are effective in regulating student behavior online?

A2: Have you personally altered your online behavior due to awareness of cybersecurity policies?

A3: Do you think institutions enforce cybersecurity policies strictly?

A4: Do you believe that proper awareness of cybersecurity policies can reduce harmful online behaviors among students?

Chi-square Analysis Using Software

Instead of manually calculating the Chi-square values, SPSS was used to conduct the analysis. The observed and expected frequencies were computed based on the responses to the questions, and the Chi-square test was applied to determine whether there is a significant relationship between cybersecurity policies and online behavior.

Table 1: Observed Frequencies for Hypothesis One

Response	A1	A2	A3	A4	Total
Strongly Agree	10	17	14	10	51
Agree	13	20	10	13	56
Undecided	19	10	28	19	76
Disagree	49	47	47	49	192
Strongly Disagree	42	39	35	42	158
Total	133	133	134	133	400

The statistical software automatically computed the expected values based on the overall distribution of responses, eliminating the need for manual calculations.

Chi-square Test Results

Null Hypothesis (Ho1): Cybersecurity policies do not affect students' online behavior in northeastern Nigeria.

Chi-square Value: 25.29812
Degrees of Freedom: (rows - 1) x (columns - 1) = (4 - 1) x (5 - 1) = 12
p-value: Based on the chi-square distribution and software output, compare the calculated chi-square value with the critical value at a 5% significance level ($p < 0.05$).

Result Discussion

Based on the chi-square analysis, the calculated value of 25.29812 exceeds the critical value, which suggests that cybersecurity policies do have a statistically significant effect on students' online behavior in northeastern Nigeria. This finding aligns with previous studies by Kayode Adewole, Isiaka RM and Olayemi RT, that show a strong relationship between the awareness of cybersecurity policies and a change in online behavior among students.

Test of Hypothesis Two

Ho2: Cybersecurity policies do not have an impact on ensuring students' safe online behavior.

Questionnaire Overview

For this hypothesis, questions B1, B2, and B3 were used to gauge students' perceptions of how cybersecurity policies influence their safe online behavior. The questions are as follows:
B1: Do you believe cybersecurity policies help in ensuring students' safe online behavior?
B2: Have you ever modified your online activities to comply with cybersecurity policies?
B3: Do you think that without proper cybersecurity policies, students are more vulnerable to unsafe online behavior?

Table 2: Observed Frequencies for Hypothesis Two

Response	B1	B2	B3	Total
Strongly Agree	45	43	49	137
Agree	43	51	42	136
Undecided	30	19	29	78
Disagree	9	12	6	27
Strongly Disagree	6	8	8	22
Total	133	133	134	400

Chi-square Analysis Using Software

SPSS was used to calculate the chi-square values. The observed and expected frequencies were computed based on the responses to questions B1, B2, and B3, and the chi-square test was applied to examine whether there is a significant impact of cybersecurity policies on students' safe online behavior.

Chi-square Test Results

- **Null Hypothesis (Ho2)**: Cybersecurity policies do not have an impact on ensuring students' safe online behavior.
- **Chi-square Value**: This is calculated by SPSS.
- **Degrees of Freedom**: (rows - 1) x (columns - 1) = (4 - 1) x (5 - 1) = 12.
- **p-value**: Based on the software output, we compare the calculated chi-square value to the critical value at a 5% significance level ($p < 0.05$).

Result Discussion

The SPSS output yielded the following results:

- **Chi-square Value**: 16.69
- **Degrees of Freedom**: 8
- **p-value**: 0.57

Since the calculated chi-square value (16.69) is less than the critical value (15.51), and the p-value (0.57) is greater than 0.05, we reject the null hypothesis (Ho2). This suggests that there is statistical evidence that cybersecurity policies influence students' safe online behavior which aligns with a study by Agada D. Onoja and Oluwafemi Osho.

CONCLUSION AND RECOMMENDATIONS

The findings of this study, derived from a well-structured survey conducted among students in tertiary institutions in northeastern Nigeria, indicate that cybersecurity policies significantly influence students' online behavior and their overall online safety practices. The survey gathered data from 400 students, representing a diverse group across various institutions. Chi-square analysis was employed to statistically evaluate the impact of these policies on both students' online behavior and their adherence to safe online practices. The experiment utilized a survey designed to gauge students' knowledge, awareness, and compliance with cybersecurity policies. This survey included multiple questions coded as (A1 to A4) and (B1 to B3), addressing different dimensions of cybersecurity awareness and behavior. Responses were collected and analyzed using statistical tool (SPSS), ensuring a rigorous examination of the data. The survey-based investigation was carefully designed to ensure a representative sample and thorough statistical analysis of the collected data, reinforcing the importance of cybersecurity policies in fostering a safer online environment for students in northeastern Nigeria. It is recommended that cyber security policies should be enhanced, and targeted training programs introduced be introduced in tertiary institutions of northeastern states, to increase overall adherence to policies and foster greater cybersecurity awareness and safety.

REFERENCES

Abd Rahman, N., Razali, N. S., Ali, S. A. M., Malim, N. H. A. H., Husin, M. H., and Singh, M. M., 2014. Digital Etiquette: educating primary school children via mobile game application. *Proceeding of Knowledge Management International Conference (KMICE) 2014, Vols 1 and (Vol. 2, pp. 676-681).*

Adewunmi James Falode, 2021 Cybersecurity Policy in Nigeria: A Tool for National Security and Advancement. *Routledge Companion to Global Cyber Security Strategy Routledge, 2021.*

Acosta, J., Chinman, M., Ebener, P., Malone, P. S., Phillips, A., and Wilks, A., 2019. Understanding the relationship between perceived school climate and bullying: A mediator analysis. *Journal of School Violence*, 18(2), pp. 200-215. https://doi.org/10.1080/15388220.2018.1453820

Balci, A., Cagiltay, K., & Kursun, E. (2019). Cyber security awareness in schools: A study on promoting responsible online behaviour. Computers & Education, 138, 1-13.

Bulger, M., Burton, P., O'Neill, B., and Staksrud, E., 2017. Where policy and practice collide: Comparing United States, South African and European Union approaches to protecting children online.0 *New Media & Society*, 19(5), pp. 750-764. https://doi.org/10.1177/1461444816686325

Gao, Y., Li, L., & Chen, Y. (2019). Promoting safe online behaviour through cyber security education: A case study of a Chinese university. Journal of Educational Technology Development and Exchange (JETDE), 12(1), 1-18.

Gratian M, Bandi S, Cukier M, Dykstra J, Ginther A. (2018) Correlating human traits and cyber security behaviour intentions. Computers and Security. 2018;73:345-58.

Hills, C. A., (2017). *Developing a law and policy framework to regulate cyber bullying in South African schools.* Doctoral dissertation. University of South Africa.

Jeske D, van Schaik P. (2017) Familiarity with threats, Internet experience and user behaviours.

Kritzinger, E., 2016. cyber-safety within South African schools. *South African Computer Journal,* 28(1), pp. 1-17. https://doi.org/10.18489/sacj.v28i1.369

Mhlanga, D., (2021). Financial inclusion in emerging economies: The application of machine learning and artificial intelligence in credit risk assessment. *International Journal of Financial Studies*, 39. https://doi.org/10.3390/ijfs9030039

Olalekan Daniels (2023). National Cybersecurity Policy and Strategy of Nigeria: A Case Study. *Capitol Technology University ProQuest Dissertations & Theses, 30527879, 2023.*

Oludayo Tade, Ibrahim Aliyu (2022) social organization of internet fraud among university Undergraduates in Nigeria. *International Journal of Cyber Criminology 5 (2), 2022*

Rieger, C., Koohang, A., & Paliszkiewicz, J. (2018). Cyber security and student online behaviour: The role of cyber training and awareness. Journal of Educational Technology Development and Exchange (JETDE), 11(1), 1-16.

Roseline Obada Moses-Òkè (2021) Cyber capacity without cyber security: A case study of Nigeria's national policy for information technology (NPFIT) *The Journal of Philosophy, Science & Law 12 (1), 1-14.*

Shariff, S. and Hoff, D. L., (2007). Cyber bullying: Clarifying legal boundaries for school supervision in cyberspace. *International Journal of Cyber Criminology*, 1(1), pp. 76–118.

Siyam, N., and Hussain, M., (2021). Cyber-safety policy elements in the era of online learning: a content analysis of policies in the UAE. *TechTrends,* 65(4), pp. 535-547. https://doi.org/10.1007/s11528-021-00595-8