Journal of Social Sciences and Educational Practices (JSSEP)
Website:https://journal.vu.edu.pk/JSSEP
Email: jssep@vu.edu.pk
Faculty of Education
Virtual Universtiy of Pakistan

Vol. 2, No. 1, 1-13, 2026
e-ISSN: 3106-6488

Knowledge and Attitude Towards Cybersecurity Education Among Pre-Service Business Education Teachers in Colleges of Education in Southwest Nigeria

Bilqees Mopelola Oladunni-Mohammad[1], Olajumoke Omojuwura Onifade[2]

Department of Technology and Vocational Education
Faculty of Education
University of Lagos

Abstract

This paper examines pre-service teachers of business education in federal colleges of education in Southwest Nigeria on cybersecurity knowledge and attitudes. With the penetration of digital technologies into learning settings, the topic of cybersecurity literacy has ceased to be a technical issue to be considered as a social priority. The study used a survey design that was descriptive and involved 149 pre-service teachers in the three federal colleges of education and utilized Cybersecurity Knowledge and Awareness Questionnaire (CKAQ) to gather the information. The theoretical model incorporated Technology Acceptance Model, Knowledge-Attitude-Practice Model, and Protection Motivation Theory to study the views of the participants towards cybersecurity education. The results showed that 87.2 percent of the respondents knew about cybersecurity education and 12.8 percent indicated that they did not know about cybersecurity education. Attitude analysis based on the three dimensions of anxiety (mean=2.56), confidence (mean=2.61) and likeness (mean=2.64) revealed moderate levels in all groups indicating that there was no evidence of strong enthusiasm or resistance of cybersecurity education. The demographics revealed that most of the participants were females (61.7) and that Marketing (45) and Accounting Education (43.6) are the main evolution paths. This paper finds that pre-service business education teachers, on the whole, acknowledge the significance of cybersecurity, but perceive it differently with some confidence. Systematic curriculum integration, differentiated instructions, and teacher educator professional development and institutional policy support are some recommendations that need to be made to advance cybersecurity education in teacher preparation programs. Such steps would make future business educators more prepared to promote digital resilience in their classrooms and make Nigerian education a safer digital system.

Keywords*:* Cybersecurity education, Pre-service teachers, Business education, Digital literacy, Teacher preparation.

Citation

Oladunni-Mohammad. B. M., & Onifade. O. O. (2026). Knowledge and Attitude Towards Cybersecurity Education Among Pre-Service Business Education Teachers in Colleges of Education in Southwest Nigeria. *Journal of Social Sciences and Educational Practices*, 2(1), 1-13.

[1] Corresponding Author. Department of Technology and Vocational Education, University of Lagos.
Email address. mopelolamohammed15@gmail.com

Introduction

Cybersecurity has become a critical support of digital transformation of education and business in the 21st century (Ayanwale, Sanusi, Molefi, and Otunla, 2024). With the increased reliance of the digital systems by societies, people are more vulnerable to a range of cyber-attacks, including phishing, identity theft, ransomware, information breaches, and cyberbullying. This fact has transformed cybersecurity education into a societal issue, especially in educational institutions where young digital natives are being trained to meet the requirements of a technology-driven society (Apata, Adeniyi, Ajiwoju, and Adeosun, 2025; Ameen, Liu, and Ahmad, 2021). According to World Economic Forum (2022), cybersecurity threats are changing faster than ever and human error contributes to over 90% of breaches, which is why education plays an essential role in ensuring safety on the Internet. The teachers (especially the novice ones) should also be well prepared not only with the minimum ICT proficiency, but also with effective knowledge of digital ethics, cyber hygiene and online risk management (Chigada & Madzinga, 2021). Being professional in the future, the teachers of pre-service business education are anticipated to act as knowledge conveyors as well as role models of safe digital practices in classrooms as well as in the workplaces.

The increased use of cybersecurity literacy is heightened in Nigeria due to the increased penetration of digital technologies in instruction and learning. The government strategies like National Digital Economy Policy and Strategy (202030) have focused on developing digital skills, in all directions of education. Nevertheless, policy and implementation are now more distant, especially in teacher preparation programs (Tew, 2019). Though ICT modules are implemented in the curriculum of many colleges of education, training in cybersecurity has shortages or has not been introduced at all (Ayanwale et al., 2024). This is worrisome, however, considering the growing dependence on internet-based methods of research, teaching, evaluation and communication.

Moreover, business education teachers in Nigeria working in pre-service are two areas which are particularly susceptible to cybercrime. Their duality requires them to possess a pedagogical and practical understanding of principles of cybersecurity including data privacy, safe online transactions, and social media responsible use. However, not many empirical studies have evaluated the preparedness of these future educators to overcome such risks (Olusola and Ayo, 2021). The absence or insufficient level of cybersecurity sensitivity or the inappropriate attitude to digital safety may not only jeopardize their own professional integrity but also the safety of their students as well as the future employers.

The research in the world has demonstrated that cybersecurity attitudes play a significant role in influencing the behavioral intentions and adoption of safe practices (Ameen et al., 2021). Resistance will occur due to negative emotions such as fear, anxiety, or skepticism, whereas engagement will be enhanced by confidence and positive experiences. Such a duality necessitates an assessment of the knowledge as well as the attitudinal preposition of pre-service teachers to cybersecurity education. This paper thus examines the cybersecurity knowledge level and the pre-service business education teachers attitude towards cybersecurity education in federal colleges of education in Southwest Nigeria. The knowledge obtained after this research will be used to give evidence-based suggestions to curriculum developers, teacher educators, and policymakers and will help them design responsive training programs that will enable future educators to operate safely and ethically in the digital age.

Problem Statement

The problem of cybersecurity threat is growing around the world, impacting not only businesses and government but also institutions of learning. The importance of cybersecurity education is increasingly important as the application of digital tools becomes commonplace in the Nigerian classrooms. Business education, which incorporates the use of ICT puts pre-

service teachers at the center of utilizing digital interactions. Nevertheless, there are concerns about the readiness of them to navigate, comprehend and educate the threats of cybersecurity. The initial observations indicate that although pre-service teachers engage with digital tools almost every day, they are not fully aware of cybersecurity and the attitude towards cybersecurity training is unclear. These future educators can be left helpless to protect themselves, their students and their institutions against cyber threats without proper knowledge and a good attitude towards cybersecurity.

Moreover, the existing teacher education curriculum does not seem to be focused on cybersecurity training to a large extent. The existence of this gap raises the issue of the preparedness of pre-service teachers to form a part of safe and informed digital learning conditions. The given study, thus, aims to address this gap in knowledge by determining the level of cybersecurity knowledge and attitude of pre-service business education teachers towards cybersecurity education among the sampled federal colleges of education in Southwest Nigeria.

Theoretical Framework

This paper is grounded in three theories which are closely linked to each other: the Technology Acceptance Model (TAM), the Knowledge-Attitude-Practice (KAP) Model, and the Protection Motivation Theory (PMT). These theories can be collectively used to create a holistic approach to the study of cybersecurity knowledge and attitudes of pre-service business education educators in Nigerian Colleges of Education.

1. Technology Acceptance Model (TAM) Technology Acceptance Model developed by Davis (1989) holds that there are two key variables namely Perceived Usefulness and Perceived Ease of Use which determine the attitude of users towards a technology which in turn affects their behavioral intention to use and actual use. This model has been popular in the educational technology studies to describe the process of implementing new digital practices by teachers and learners (Ameen, Liu, and Ahmad, 2021). The TAM can be utilized in this study to understand how the beliefs of pre-service teachers regarding the relevance and usability of cybersecurity knowledge affect their attitudes towards cybersecurity education and readiness to use cyber-safe practices.

2. Knowledge-Attitude-Practice (KAP) Model. KAP model is a behavioral model, which indicates that when knowledge is acquired, it forms an attitude, which in turn affect practices or behavior. This paradigm has been commonly applied in researches on public health and information security in understanding individual responses to risks and protective action (Chigada & Madzinga, 2021). The KAP model will be applicable in this study because the model will be used to support the supposition that enhancing the cybersecurity awareness of pre-service teachers will have a positive impact on attitudes and lead to improved digital safety behaviors in schools.

3. Protection motivation theory (PMT) The Protection Motivation Theory, which is proposed by Rogers (1975), explains that people take protective action (e.g. cybersecurity practices) depending on the threat appraisal (perceived severity and vulnerability) and coping appraisal (response efficacy and self-efficacy). PMT has been applied in education to investigate the reaction to cyber threats and preventative strategies among the participants (Olusola and Ayo, 2021). In this research, PMT helps understand that the perception of cybersecurity risks by pre-service teachers along with their attitude to their competence to react efficiently determine their motivation to practice safe online behavior.

Purpose of the study:

The main purposes of this study is to examine knowledge and attitude towards cybersecurity education among pre-service business education teachers in colleges of education in southwest Nigeria. Specifically, the study examined:

1. Knowledge of cybersecurity education among pre-service business education teachers in colleges of education.
2. Attitude of pre-service business education teachers in colleges of education towards cybersecurity education.

Research Questions

The following research questions were explored.

1. What is the level of knowledge of cybersecurity education among pre-service business education teachers in colleges of education?
2. What is the attitude of pre-service business education teachers in colleges of education towards cybersecurity education?

Methodology

Research Design

A descriptive survey research design was selected in this study because it is suitable in gathering information about the current situations, practices, and opinions without interfering with the variables. The descriptive survey design was chosen as it will enable the researcher to gather a lot of data about the knowledge, awareness, and attitudes of pre-service Business Education teachers in Southwest Nigeria as far as cybersecurity education is concerned.

Area of the Study

The study was carried in Southwest geopolitical region of Nigeria comprising of States of Oyo, Ogun, Ekiti, Ondo, Osun and Lagos. The area is also renowned to have various Colleges of Education and also provide a large number of qualified teachers. Three federal Colleges of Education have been chosen in the frame of this research purposely:

• Federal College of Education (Technical), Akoka, Lagos state.
• Federal College of Education, Osiele, Ogun State.
• Federal College of Education (Special), Oyo, Oyo state.

The predominant factor as to why these three (3) Federal Colleges of Education was chosen is due to the fact that other Colleges on Education in the Southwestern region are now Universities of Education and are also State owned Institutions.

Population of the Study

The population of interest was 212 pre-service teachers in Business Education who were enrolled in the federal Colleges of Education selected in the 2024/2025 academic session. These respondents were selected out of the School of Technical Vocational Education, which is the ones enrolled in Business Education courses. Sample and Sampling Technique. The three federal Colleges of Education were chosen using the purposive sampling method, according to their relevance and programs. A complete population participation was observed since all 212 pre-service Business Education students of these colleges were used as the sample of the study. The institutional records that served as a guide to the sampling were those that existed during the 2023/2024 academic session.

Table 1

Distribution of Stakeholders in College of Education

S/N	Colleges of Education	Students	Sampled Facilitators
1	Federal College of Education (Special), Oyo	83	52
2	Federal College of Education, Osiele, Abeokuta	72	37
3	Federal College of Education (Technical) Akoka	57	62
Total		212	149

The sample of stakeholders in the two Federal Colleges of Education identified in Southwest Nigeria indicates that the sampling of the participants in this research was strategic. The total number of pre-service Business Education students enrolled in the three sampled colleges was 212 and a sample population of 149 was selected among them due to their availability in the College as at the time the research was conducted. There are 83 registered Business Education students in the 2023/2024 academic session at the Federal College of Education (Special), Oyo. This number was reduced to 52 students who were sampled to take part in the study. This institution formed a significant part of the total sample as it represented about a third of the respondents. It has been chosen so because it has had a long-standing record in teacher education, especially in special education and vocational studies.

The Federal College of Education, Osiele, Abeokuta, had a sample of 37 students of Business Education out of a total population of 72 students. Even though student population was a bit smaller than that of Oyo, inclusion of the student population in the study was needed to have a balance representation throughout the region. The sampling figure represents approximately one quarter of the entire participants of the study. On the other hand, Federal College of Education (Technical), Akoka, even though it had the lowest overall student population of the three (57 students), provided a sample size of 62. This bias indicates that the sample may have contained not just students but there could be other participants such as facilitators or other subjects that are pertinent to the study. The high attendance rate of Akoka identifies a great involvement of the college in the use of technology-based education which resonates well with the purpose of the study which aims at cybersecurity education. In short, out of a population of 212 pre-service business education teachers in three federal Colleges of Education in Southwest Nigeria, 149 respondents were selected purposely to represent the entire sample of 149 pre-service business education teachers since 149 are the only available and the only available respondents to the research.

The sampling was done to guarantee a wide and extensive distribution of sampling, which increases the validity of the findings and gives a substantial background to study knowledge and attitudes towards cybersecurity education among future educators in the area.

Research Instruments

This paper employs two properly designed research tools to adequately assess the knowledge and awareness level of pre-service Business Education students on cybersecurity. The main tool, which is called the Cybersecurity Knowledge and Awareness Questionnaire (CKAQ), consists of the sections starting with demographic data and then with detailed items of evaluating the level of cybersecurity knowledge and awareness of participants. To measure the perceptions and the perception of the respondents accurately and consistently regarding the issues of cybersecurity, the questionnaire is based on 4-point Likert scale, which is Strongly Agree (4), Strongly Disagree (1).

Methods of Data Collection

The researcher received a letter of introduction to her department in order to have an easy time in collecting the data. Having this in hand, she would go to each of the chosen Federal Colleges of Education, and seek official authorization to engage their students in the study. All targeted participants were informed and therefore gave their consent before the administration of the instrument in order to participate willingly. Moreover, a concise description of the purpose of the study was put on the first page of the questionnaire to keep the respondents informed. After receiving permission, the selection of the participants was done following the sampling procedure outlined in the previous section under Sample and Sampling Techniques. The researcher informed the sampled pre-service teachers about the aims and the objectives of the study and then administered the questionnaire. Two research assistants were hired in each of the participating colleges to help in the data collection process. These assistants were informed about the purpose of the study and given one day training about the correct procedure

on how to administer the instrument and how to approach the participants. The questionnaires were then administered and the researcher collected them, with the help of the trained research personnel.

Methods of Data Analysis

Quantitative methods were used to analyse the data that was collected in the present study. Responses were summarized and interpreted by use of descriptive statistics such as frequency counts, percentages, means and standard deviations to answer the research questions. Inferential statistics, to be more precise, multiple regression analysis was implemented with the level of significance of 0.05 to test the hypothesis of the research. This method helped the researcher to detect patterns and relationships in the data, advising the researcher a thorough insight into the variables being investigated.

RESULT

Table 2

Respondents from Federal Colleges of Education

S/N	Colleges of Education	Sampled	%
1	Federal College of Education (Special), Oyo	52	34.44
2	Federal College of Education, Osiele, Abeokuta	37	24.50
3	Federal College of Education (Technical) Akoka	62	41.06
Total		149	100

Table 2 presents the distribution of respondents drawn from three Federal Colleges of Education in Southwest Nigeria. The Federal College of Education (Special), Oyo, accounted for 52 participants, representing 34.44% of the total sample. This reflects a considerable contribution to the overall dataset. The Federal College of Education, Osiele, Abeokuta, contributed 37 participants, which constitutes 24.50% of the total respondents—indicating a moderate level of representation. Meanwhile, the Federal College of Education (Technical), Akoka, recorded the highest participation with 62 respondents, making up 41.06% of the sample. Altogether, the three institutions yielded a total of 149 respondents. The distribution underscores a balanced and inclusive approach to data collection, with each college contributing proportionally to ensure diverse perspectives within the study population.

Table 3

Respondents based on Course of Study

S/N	Course of Study	F	%
1	Accounting Edu	65	43.6
2	OTME	7	4.7
3	Marketing	67	45.0
4	Entrepreneurial	10	6.7
	Total	149	100

Table 3 highlights the distribution of respondents according to their respective courses of study. Out of the total 149 participants, Marketing recorded the highest number of students, with 67 respondents, accounting for 45.0% of the sample. This was closely followed by Accounting Education, which had 65 students, representing 43.6%. These two courses clearly dominate the academic landscape among the respondents. In contrast, Entrepreneurial Studies had 10 students (6.7%), while Office Technology and Management Education (OTME) had the fewest participants, with 7 students (4.7%). Collectively, students in Marketing and Accounting Education constituted 88.6% of the total sample, indicating a significant concentration in these areas of specialization.

Table 4

Respondents based on Gender

S/N	Gender	F	%
1	Male	57	38.3
2	Female	92	61.7
	Total	149	100

Table 4 presents the gender distribution of the 149 respondents in the study. Female participants constituted the majority, numbering 92 and representing 61.7% of the total sample. Male respondents accounted for 57 participants, making up 38.3% of the total. This reveals a significant gender imbalance in favor of female students, with a ratio of nearly three females to every two males.

Research Question 1: Are pre-service business education teachers in colleges aware of cybersecurity education

Table 5

S/N	Statement	Aware F (%)	Not Aware F (%)
1.	I am aware of cybersecurity education	130 (87.2)	19 (12.8)

The findings reveal that a substantial proportion of pre-service business education teachers are aware of cybersecurity education. Out of the total respondents, 130 (87.2%) acknowledged their awareness, while only 19 (12.8%) reported being unaware. This indicates that the vast majority of participants have some familiarity with cybersecurity education. However, the small but notable percentage of respondents lacking awareness highlights the need for further efforts to ensure comprehensive understanding across all pre-service teachers.

Research Question 3: What is the attitude of pre-service business education teachers in colleges of education towards cybersecurity education

Table 6

S/N	Statement	Means	SD
	Anxiety		
1.	Cybersecurity education does not scare me at all	2.63	1.50
2	Cybersecurity would make me nervous online	2.48	1.46
3	I do not feel threatened when others talk about cybersecurity	2.57	1.26
4	I do not feel aggressive and hostile towards cybersecurity	2.63	1.41
5	It wouldn't bother me at all to take Cybersecurity courses	2.50	1.44
6	Cybersecurity makes me feel uncomfortable	2.38	1.48
7	I would feel at ease in a Cybersecurity class	2.84	1.55
8	I feel uncomfortable working online without considering cyber threats	2.60	1.47
9	Cybersecurity makes me feel uneasy and confused	2.41	
	Confidence		
10	I am not good at tackling Cybersecurity issues	2.50	0.37
11	Generally, I would feel okay about trying a new technology without threat	2.88	0.33
12	I can do advanced work amidst Cybersecurity	2.53	1.50
13	I am sure I could learn Cybersecurity language	2.83	1.46
14	I could get good grades in Cybersecurity courses	2.63	1.25
15	I do not think I could handle Cybersecurity course	2.24	1.41
16	I have a lot of confidence when it comes to working with online	2.63	1.44
	Likeness		
17	I would like to have more knowledge about Cybersecurity	2.81	0.33
18	The challenge of solving problems with Cybersecurity does not appeal to me	2.53	1.50

19	I think understanding Cybersecurity would be enjoyable	2.67	1.46
20	Cybersecurity problems does not appeal to me	2.67	1.25
21	When there's a problem on Cybersecurity that I can't immediately solve, I will stick with it until I have the answer	2.57	1.41
22	Once I start to work with Cybersecurity, I will find it hard to stop	2.63	1.44
23	If a problem is left unsolved in a Cybersecurity case, I would find it hard to continue to think about it afterward	2.59	1.48
24	I do not enjoy talking with others about Cybersecurity	2.34	1.55
25	I do not enjoy talking with others about Cybersecurity	2.92	1.47

Average Mean: The mean score is 2.50
Anxiety: The average mean is approximately **2.56**.
Confidence: The average mean is approximately **2.61**.
Likeness: The average mean is approximately **2.64**

The research analysed the pre-service business education teachers attitudes towards cybersecurity education in three dimensions which include anxiety, confidence and likeness. The results show that the neutral to moderately positive attitude towards cybersecurity education is observed among respondents in general. In terms of anxiety levels, the average mean of 2.56 indicates that the anxiety level is moderate. There were participants who felt comfortable with the concept of cybersecurity - as it can be seen that the levels of agreement with statements such as I would feel at ease in a Cybersecurity classroom (2.84) and Cybersecurity education does not scare me at all (2.63) are higher - but there were also those who felt discomfort. This is shown through less score on issues like Cybersecurity makes me feel uncomfortable (2.38) and Cybersecurity makes me feel uneasy and confused (2.41) issues. The standard deviations (1.26 to 1.55) between these items of anxiety-related anxiety are relatively high which can be said to mean that there is a high level of variation in individual responses as some teachers are confident with cybersecurity, whereas others show considerable anxiety.

The confidence dimension had an average mean of 2.61 which implied that there were moderate self-assurance levels among the respondents. The participants were most confident with their possibility to learn the concepts of cybersecurity (I am sure I could learn Cybersecurity language - 2.83) and in working with new technologies (Generally, I would feel okay about trying a new technology without threat - 2.88). Nonetheless, a number of respondents had their doubts regarding their abilities especially in managing advanced cybersecurity coursework (I do not think I could handle Cybersecurity course - 2.24). The relative average confidence rates, combined with the difference in answers, indicate that although a large number of pre-service teachers are confident in their ability to acquire cybersecurity skills, some of them might need further assistance and inspirations. Regarding the similarity or interest towards cybersecurity, the average score of 2.64 shows the slight yet positive inclination. The most interest was shown in gaining more cybersecurity knowledge (2.81) and the least interests were shown in enjoying the discussion of cybersecurity topics with others (2.34 and 2.92, but the latter score seems to be anomalously large and should be confirmed). The average ratings in persistence in solving cybersecurity problems (2.57) and enjoyment of cybersecurity challenges (2.67) indicate that most respondents have a perceived benefit in cybersecurity education but lack passion in it because they view it as challenging or not necessarily relevant to their current teaching products.

All the findings point to the general conclusion that pre-service teachers of business education seem to be aware of the significance of cybersecurity education but feel more or less comfortable and confident about it. The medium results in all three dimensions show that there is no high enthusiasm or strong resistance, just a wary openness to cybersecurity training. The profile of the attitude indicates that those training programs that are designed in a supportive manner can work effectively on improving the competence and confidence of cybersecurity

issues of these future educators. The gap in the responses shows that there is a necessity to use differentiated instructional strategies that will be able to support the different levels of comfort and learning needs of this population.

Discussion of Findings

The study is informative in terms of understanding of awareness and attitudes of pre-service business education teachers towards cybersecurity education in three Federal Colleges of Education in Southwest Nigeria. The results uncover significant trends that should be given a second thought when the teacher training and curriculum design are concerned. The respondent demographics indicate that the sample of respondents was representative of three major institutions with Federal College of Education (Technical) Akoka having the highest number (41.06%), then Federal College of Education (Special) Oyo (34.44%) and Federal College of Education, Osiele Abeokuta (24.50%).

This dispersion guarantees the geographic distribution and institutional representation in the study area. It is important to note that Marketing (45%) and Accounting Education (43.6) students were the most represented in the sample, and other students majoring in business education were underrepresented significantly. Such imbalance could indicate existing trends in enrollment, or areas of institutional focus, so that cybersecurity education programs may have to be customized differently in different business education fields. Another positive observation is the extent of cybersecurity knowledge among the respondents with 87.2 percent stating that they are aware of the concept. This indicates that cybersecurity learning is being embraced in teacher education degree programs, perhaps via structured education or unstructured exposure to digital security matters.

Nevertheless, the other 12.8% that said that they were not aware is a dangerous hole that cannot be left unsealed because these future educators might not have the necessary information to demonstrate and impart safe online habits to their students. The attitudes assessment based on three important dimensions, such as anxiety, confidence, and likeness, allows seeing a rather complicated image of how pre-service teachers are ready to participate in cybersecurity education. The fact that moderate levels of anxiety (mean = 2.56) align with the idea that many respondents are not afraid of the concept of basic cybersecurity, but it seems that a considerable number of them feel out of their comfort zone, especially regarding the more technical elements. This is supported by a big diversity of reactions to the anxiety-related statements as some participants said that they felt relaxed when classes were hypothetically discussed on cybersecurity and others said they felt uncomfortable and confused. The same cautious optimism is reflected in the levels of confidence (mean = 2.61).

There was a fair amount of confidence in the skills of the respondents to master the basics of cybersecurity but much lower confidence in regards to high-level applications. Such dichotomy implies that, although pre-service teachers are aware of the need to be cybersecurity literate, they have a feeling that they might be deficient in technical expertise. The most promising results might be the dimension of likeness (mean = 2.64) since respondents have shown moderate interest in learning more about cybersecurity. Nonetheless, the reduced scores on the questions associated with collaborative learning and the problem-solving indicate that there can be a decrease in engagement when cybersecurity is framed as socially interactive or intellectually challenging. This lays the emphasis on pedagogical solutions to enable future business educators to make cybersecurity learning more accessible and engaging. The implications of these findings to teacher education programs are significant.

The difference in the attitudes implies that a universal model of cybersecurity education can be inefficient. Rather, differentiated instruction which recognizes the differences in the anxiety and confidence levels would show higher results. Learning activities that are more practical and hands-on may contribute to the demystification of the concept of cybersecurity, whereas collaborative activities may eliminate the unwillingness to engage in the subject matter

demonstrated by some respondents. The gender imbalance of the sample (61.7% female) creates intriguing questions regarding the possible gender disparity in cybersecurity attitude that could be evaluated in the future research. Likewise, the result of concentrating respondents in the Marketing and Accounting Education programs is that some studies are required to explore attitudes in a wider scope of business education specialization. Although this paper gives important background information, its scope is restricted to three colleges within a single area which restricts the extrapolation of results.

Further studies would be able to increase the number of geographic areas and different types of institutions. It would also be of great value to conduct longitudinal studies to follow the changes in attitudes in relation to exposure to cybersecurity education. To sum up, this paper shows that pre-service business education teachers in Southwest Nigeria have overall awareness of the need to teach cybersecurity and do so with a range of apprehension and confidence. The results are indicative of the fact that effective, supportive training programs may be an effective way to raise the level of competence and confidence regarding cybersecurity issues among these future educators. With the mentioned gaps in the understanding and attitudes filled, teacher training programs will be able to equip business educators to promote the creation of digital resilience in their classrooms and help to make the Nigerian education system more secure and less reliant on digital threats.

Conclusion

The research has generated a lot of information on the level of awareness and the attitude of pre-service business education teachers to cybersecurity education in three Federal Colleges of Education in Southwest Nigeria. The results offer some positive trends and valuable issues, which should be taken into consideration when developing teacher education curricula. The study shows that there is a high level of cybersecurity awareness among the respondents with 87.2% of the respondents stating that they were familiar with the concept. Such a high awareness rate implies that cybersecurity training is slowly becoming a topic of teacher preparation programs, either through formal coursework or more generally exposing the society to the topic of digital security. Nevertheless, the other 12.8% who indicated that they were not aware of it is also a limiting gap that should be filled by policy-makers of education since these teachers will be tasked with leading and teaching the practices of digital safety to their students. Attitude analysis in three different dimensions, including anxiety, confidence, and likeness, indicates a complex view of the willingness of the pre-service teachers to use cybersecurity education. The average values of anxiety (2.56) show that most of the respondents are not afraid of most fundamental ideas of cybersecurity, but a good number is afraid especially when the technical side is involved.

This difference in levels of comfort implies that the process of cybersecurity education among teachers requires differentiation in teaching. Likewise, the dimension of confidence (mean = 2.61) exhibits the tendency of cautious optimism, with the respondents being fairly confident in their skills to study the basic concepts of cybersecurity but being much less confident when dealing with advanced applications. This fundamental and sophisticated competency perception dichotomy brings up a critical issue of teacher education programs in how to organize suitable cybersecurity content. The most prospective results arise in the likeness dimension (mean = 2.64), as there respondents were more or less interested in getting more knowledge about cybersecurity. This good attitude, together with the high awareness rates, provides a good support base on which cybersecurity education can be incorporated in teacher preparation education. The lower scores of collaborative aspects of learning, however, indicate that the approach to the practice must focus more on practical, involving practice, instead of focusing on theoretical or socially-intensive models.

These conclusions are further informed by the demographic results of the study. The skewed distribution of female respondents (61.7%), which is consistent with the general

tendencies in the teacher education programs, may be the reason to consider gender-specific ways of teaching cybersecurity. On the same note, the homogenization of respondents in the Marketing and Accounting Education programs (88.6% combined) may imply that cybersecurity education programmes should be tailored to the specifics of disciplines and their curricular requirements and backgrounds of students. The implications of these findings on the policy and practice of teacher education are significant. The awareness and overall positive attitudes provided prove that the teaching community is open to cybersecurity education, yet the difference in the confidence and anxiety rates proves that the implementation should be well-thought out. The teacher education programs should take into consideration:

1. Creating different cybersecurity programs that suit different degrees of comfort and competency.
2. The use of practical learning, involving the use of hands-on learning.
3. Developing discipline-specific adaptations of various business education specializations.
4. Considering gender in instructional design.
5. Having specific interventions to those who are in the minority and are not well-informed in cybersecurity. Although, the present research is quite insightful, the fact that it is limited to three colleges in a single region indicates the necessity to conduct more extensive research in order to validate and generalize the results. Future research may look at: - The practice of various pedagogical strategies in teaching cybersecurity to teachers. - Attitudinal changes with longitudinal tracking of the training programs. - Comparative studies in various regions and types of institutions. - The correlation between pre-service training and ultimate classroom application.

To sum up, this study confirms that teachers of pre-service business education in Southwest Nigeria overall are familiar with and have a positive orientation toward cybersecurity education with a moderate degree of confidence and comfort. The findings provide not only a chance but also a challenge to teacher education programs that aim to equip teachers with the digital era. Through the expansion of the current awareness and already established positive dispositions as well as filling the identified gaps and variations, the Nigerian teacher education can devise successful strategies to arm future teachers in business management with the necessary knowledge and skills of cybersecurity in the 21st century classrooms. Not only will the effective inclusion of cybersecurity training in the educator training benefit them directly, but it will eventually lead to the creation of a more digital and secure society by way of their future learners**.**

Recommendations

According to the findings of the study, the set of the following recommendations can be offered to improve cybersecurity training among the pre-service business education teachers in the colleges of education in Nigeria:

1. Curriculum and Pedagogical Strategies: In order to support the differences in awareness and confidence, cybersecurity training must be methodically included in the curriculum of teacher training. Instead of making it their own specialty, the cybersecurity concepts must be incorporated in other pertinent courses of business studies or programs, like Accounting, Marketing, and Office Technology. A structural design might be implemented, starting with basic computer skills and then moving on to the principles of advanced cybersecurity. The following should be the priority of the pedagogical strategies: Practical, real-life learning (e.g. simulation of phishing attacks or data breach) to de-techno-fy the technical. Different instruction to meet the needs of different levels of anxiety like optional advanced classes to students who are interested. Group projects that promote learning between peers to overcome the unwillingness of some respondents to engage in group discussions.
2. Professional Development of Teacher Educators: The middle level of confidence of many pre-service teachers can also indicate that the faculty members might also need training to teach

cybersecurity material. Colleges of education are recommended to: Provide teacher educator workshops on the basics of cybersecurity and pedagogy. Collaborate with professionals in the industry and IT specialists to co-teach specialized content to make it relevant to business realities. Create open educational resources (OERs) including case studies and lesson plans specific to the field of business education.

3. Dealing with Gender and Disciplinary Gap: Since there is a gender imbalance (61.7% of the respondents were female), and the preponderance of the Marketing and Accounting students, some special work is required: The possible differences in confidence or engagement would be addressed in gender-sensitive workshops to make sure that female educators have the same power to teach cybersecurity. Individual, discipline-related examples (e.g. securing financial data as an Accounting student or risk of digital marketing as a Marketing student) would be more relevant and interesting. Encourage underrepresented fields (e.g. Entrepreneurial Studies, OTME) to participate by offering a scholarship or certification.

4. Institutional/Policy Support: In order to maintain cybersecurity education, the institutional commitment is essential: Protect business courses in national teacher education standards through mandate cybersecurity modules. Invest in cybersecurity labs, software and talks by industry experts. Create student cybersecurity clubs so that there is peer mentoring and practical learning even beyond the classroom.

5. Future Research and Evaluation: In order to optimize such initiatives, a subsequent research must: Determine long-lasting effects of attitudinal development following the introduction of cybersecurity training. Make comparisons across the regions by expanding researches to other areas across geopolitics in Nigeria. Assess classroom results by monitoring the use of cybersecurity in classroom activities by teachers who have been trained to use it after graduation.

References

Ameen, N., Liu, H., & Ahmad, N. (2021). Closing the digital divide in the post-COVID-19 era: A review of the digital literacy landscape and policy directions. *Government Information Quarterly, 38*(4), 101620. https://doi.org/10.1016/j.giq.2021.101620

Apata, S. B., Adeniyi, J. T., Ajiwoju, J. A., & Adeosun, K. K. (2025). Digital transformation in teaching: The preparedness of in-service teachers in Nigeria for the Fourth Industrial Revolution (4IR). *British Journal of Contemporary Education, 5*(1). Retrieved from https://abjournals.org/bjce

Ayanwale, M. A., Sanusi, I. T., Molefi, R. R., & Otunla, A. O. (2024). A structural equation approach and modelling of pre-service teachers' perspectives of cybersecurity education. *Education and Information Technologies, 29*, 3699–3727. https://doi.org/10.1007/s10639-023-11973-5

Chigada, J., & Madzinga, R. (2021). Digital literacy and cybersecurity awareness among students in South African universities. *South African Journal of Information Management, 23*(1), a1292. https://doi.org/10.4102/sajim.v23i1.1292

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340. https://doi.org/10.2307/249008

Olusola, A. A., & Ayo, C. K. (2021). Cybersecurity awareness and behaviour of university students: The Nigerian experience. *Information and Computer Security, 29*(3), 402–421. https://doi.org/10.1108/ICS-02-2020-0028

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Tew, P. A. D. (2019). Cybersecurity education in Nigeria: A pre-requisite for the life-long

learner in the 21st century. *The COLLOQUIUM, 7*(1), 38–45. Retrieved from https://www.ajol.info/index.php/colloq/article/view/238718

World Economic Forum. (2022). *Global cybersecurity outlook 2022*. Retrieved from https://www.weforum.org/reports/global-cybersecurity-outlook-2022