Multidisciplinary Journal of Vocational Education & Research; Vol.8 No.1, August 2026, pg.118 - 130; ISSN(Print): 2630 – 7081

INTELLIGENCE STRATEGIES REQUIRED OF BUSINESS EDUCATION STUDENTS IN MANAGING CYBERSECURITY: A STUDY OF SELECTED TERTIARY INSTITUTIONS IN SOUTH-EAST OF NIGERIA

UBAKA, ROSELINE NKECHI
Dept. of Office Technology and Management
Federal Polytechnic, OKO
Anambra State
alamsorj@gmail.com

PROF. ANTHONIA NGOZI UMEZULIKE
Dept. of Vocational Education
Chukwuemeka Odumegwu Ojukwu University
Igbariam Campus
an.umezulike@coou.edu.ng
Phone: 07067650365

PROF JOY AMECHI OKEKE-EZEANYANWU
Dept. of Vocational Education
Chukwuemeka Odumegwu Ojukwu University
Igbariam Campus
ja.okekeze-eanyanwu@coou.edu.ng

ABSTRACT
This study examined the intelligence strategies required of business education students in managing cybersecurity in tertiary institutions in South-East, Nigeria. Two research questions and two null hypotheses guided the study. The study adopted descriptive survey research design. The population of the study comprised 521 final year students of Business Education Department from Universities and Colleges of Education in South-East. There was no sampling technique because the population was manageable. Data were collected using a structured questionnaire titled: Intelligence Strategies Required of Business Education Students in Managing Cybersecurity Questionnaire (ISRBESMCQ). The instrument was validated by three experts in the field. The reliability of the instrument was established using Cronbach Alpha method, which yielded a cumulative reliability coefficient value of 0.87. 521 copies of questionnaire were administered; 470 retrieved and used for analysis. Data was analysed using mean and standard deviation to answer research questions, and t-test statistics for testing hypotheses. The findings revealed that the students agreed that intelligent strategies applicable in managing cybersecurity

include; regular system updates, smart password management, understanding best practices in data sharing, phishing awareness, root cause analysis, continuous learning, among others. The study further found that business education students possess abilities such as manipulating cybersecurity tools, applying risk management practices, strategic thinking, effective communication, adaptability, collaboration, continuous learning, and the use of cybersecurity technologies including antivirus software, firewalls, The study concluded that effective cybersecurity management among business education students requires a combination of technical, analytical, communication, and business-related competencies. It was recommended, among others, that tertiary institutions should integrate cybersecurity intelligence strategies into the business education curriculum and provide students with practical exposure to cybersecurity tools and practices. The study contributed to the advancement of educational theory by providing empirical evidence on cybersecurity measures that can be applied to minimize cybersecurity risks.

Keywords: Intelligence strategies, cybersecurity management, business education students, cybersecurity awareness, tertiary institutions.

Introduction

The increasing dependence on digital technologies in tertiary institutions has made cybersecurity a critical concern in contemporary education. Cybersecurity refers to the application of technologies, processes, and controls designed to protect computer systems, networks, devices, applications, and data from cyber-attacks and unauthorized access. Ibrahim et al. (2024) maintained that cybersecurity involves safeguarding computer systems and networks against malicious activities that may result in data theft, destruction of hardware and software, or disruption of services. Similarly, Lindemulder and Kosinki (2024) explained that cybersecurity seeks to protect digital assets, financial resources, and users from threats, such as ransomware, phishing, malware, and data breaches. Despite its importance, Garba et al. (2020) observed that many tertiary institutions lack active programmes for improving students' cybersecurity knowledge and awareness. Similarly, the study of Edeh (2021) revealed that poor knowledge of computing areas, lack of mentors with hands-on experiences in cybersecurity, lack of supportive infrastructures, and ignorance were identified as some of the barriers that impede cybersecurity education; hence, the need for business education students to possess brilliant strategies in order to curtail activities of the unauthorised access.

Cybersecurity is essential for protecting sensitive information, preventing financial losses, and ensuring the continuity of institutional operations. Aliyu et al. (2021) found that although many students are aware of cyber threats, they often neglect important security practices such as regularly updating passwords, and exhibiting poor cyber hygiene. As cybercriminals continue to exploit technological advancements, students must develop intelligent strategies that enable them to identify, prevent, and

respond effectively to emerging cyber threats. Such competencies are necessary to protect institutional data, maintain public trust, and ensure uninterrupted academic activities. Business education students, in particular, require adequate cybersecurity knowledge because they frequently interact with digital information systems and business technologies. Payne et al. (2022) identified key aspects of cybersecurity education that students should possess, including technical competence, practical experience, lifelong learning, interdisciplinary understanding, and professional skills. These competencies enable students to protect personal and institutional information, reduce risks, and make informed decisions in a technology-driven environment. Unfortunately, there still remain weak institutional coordination; low technical capacity and limited public awareness heavily hinder effective responses to cyber threats.

A major component of cybersecurity is cyber intelligence, which involves gathering and analysing information about cyber threats, attackers, and vulnerabilities. Obiakor et al. (2025) described cyber intelligence as knowledge that helps individuals identify potential attacks, understand attackers' motives and capabilities, and take preventive actions. Intelligence in cybersecurity therefore involves the collection and analysis of real-time information from networks, applications, and users to support informed security decisions (Wadhwa, 2026). In today's digital era, where cyber threats, espionage, and cybercrime continue to evolve, intelligent cybersecurity strategies have become indispensable (Khan, 2024). This is as a result of cyber-attacks, threats like phishing, and malware which are increasingly growing among tertiary institutions and industries.

However, several studies indicated that students' cybersecurity knowledge remains inadequate. Khalid et al. (2018) reported that although university students demonstrated awareness of issues such as cyber-bullying and online banking security, many lacked sufficient knowledge of cyber self-protection. Adamu et al found that cybersecurity awareness programmes are largely absent in Nigerian tertiary institutions, resulting in deficiencies in students' understanding of password management, data protection, and other essential security practices. Similarly, the study of Wiechetek and Medrek (2023) revealed that most students reported poor or no knowledge of cybersecurity. The result of this poor knowledge of cybersecurity leaves students in data loss, financial fraud, disrupted e-learning and poor long-term digital employability.

The challenge is further compounded by the increasing prevalence of cyber threats such as phishing, malware, ransomware, and data breaches. Ogene (2024) noted that these threats frequently target Nigerian businesses and tertiary institutions. This has severe effects on them, and leads to major operational disruptions, massive financial losses; sometimes to a complete loss of customers trust. Sule et al. (2021) identified phishing, malware, and data breaches as common cybersecurity threats facing students, while Osijirin et al. (2025) reported significant gaps in students' understanding of phishing attacks, password security, and data privacy. Although business

education students generally possess basic online safety knowledge, they often lack the advanced cybersecurity awareness necessary to protect sensitive information effectively (Osijirin et al., 2026). Nevertheless, Aminu et al. (2021) found that many students are conscious of cybercrime and cyber threats, suggesting a foundation upon which more advanced competencies can be developed.

The ability to apply intelligent cybersecurity strategies is therefore crucial for business education students. Such strategies include cyber threat monitoring, threat analysis, incident response, risk assessment, and the use of actionable intelligence to prevent and mitigate cyber-attacks. Obiakor et al. (2025) emphasized that these capabilities enhance both individual and institutional resilience against cyber threats. Furthermore, Saidu et al. (2021) argued that cyber-threat intelligence is fundamental to the effective functioning of modern institutions that rely heavily on information and communication technologies.

Given the growing sophistication of cyber threats and the documented gaps in students' cybersecurity knowledge, there is a need to promote intelligent cybersecurity strategies among business education students in universities and colleges of education. Such strategies will enhance their ability to protect digital assets, respond effectively to cyber threats, and contribute to a more secure educational environment. It is against this background that this paper examines intelligent strategies applicable to managing cybersecurity among business education students in tertiary institutions.

Statement of the Problems

Cybersecurity education is scarcely new in Nigeria, though some universities such as University of Nigeria, Nsukka (UNN), University of Lagos (UNLAG), Federal University of Technology, Minna (FUTMINNA), Bayero University, Kano (BUK), among others have started cybersecurity courses and programmes. Though these universities have started these programmes, there is still insufficient cybersecurity knowledge among many university students in Nigeria. Most students know about general risks like computer viruses and social media scan, but lack practical habits like using strong password to protect their personal data, many tertiary institution students still lack adequate practical defense skills required to manage cybersecurity. Similarly, Nigerian University students are experiencing inadequate security awareness to manage cybersecurity programmes. Most of them understand basic threats but risky online behaviour is still common. While they can identify terms like phishing, or malware, researches show they routinely fail to defend against them as a result of poor awareness and insufficient knowledge. The poor security awareness means that cyber criminals and identity theft can monitor what institutions are doing online and steal both institutional passwords and personal information. With this background in mind, this paper is written in order to identify the intelligent

strategies necessary for business education students in managing cybersecurity in their various institutions.

Research Questions

The following research questions guided the study:

(i) What are the intelligent strategies applicable in managing cybersecurity?

(ii) What are the abilities of business education students in applying intelligent strategies to managing cybersecurity?

Hypotheses

The following hypotheses were tested at 0.05 level of significance:

(i) There is no significant difference in the opinions of students from federal and those of state tertiary institution on the intelligent strategies applicable in managing cybersecurity.

(ii) There is no significant difference in the opinions of students from federal and those of state tertiary institution on the abilities of business education students in applying intelligent strategies to managing cybersecurity.

Methodology

The study was carried out among selected federal and state universities and colleges of education in South East of Nigeria where business education programmes are offered, and have students at final year level as at 2025/2026 academic session. These universities and colleges of education include: University of Nigeria, Nsukka (UNN) (46), Nnamdi Azikiwe University, (NAU), Awka (102); Alvan Ikoku Federal University of Education, Owerri (88); Federal College of Education (Technical), Umunze; ((82); Alex Ekwueme Federal University of Ndufu Alike (82); Chukwuemeka Odumegwu Ojukwu University, Igbariam Campus (21); Abia State University, Uturu (07); Ebonyi State University, Abakaliki (34); Nwafor Orizu College of Education, Nsugbe (48); and Ebonyi State College of Education, Ikwo (11). The population of the study comprised 521 final year students of Business Education Department for 2025/2026 academic session. Final year students were considered suitable for the study because they have undergone enough digital skills acquisition programmes as contained in their curriculum. So they understand the importance of digital skills acquisition, computer threats, cyber threats, and changing of passwords to prevent unauthorised user from penetrating into the systems.

Instrument for data collection was a 31-item questionnaire structured by the researcher, using modified four-point rating to ascertain the

opinions of students on the strategic intelligence in managing cybersecurity. The questionnaire was structured in the following rating scale: Strongly Agreed (SA) – 4 points, Agreed (A) - 3 points, Disagreed (D) – 2, and Strongly Disagreed (SD) – 1, respectively. The instrument was validated by three experts from Business Education Department; and Measurement and Evaluation. The reliability test was conducted using Cronbach Alpha method and it yielded a cumulative reliability coefficient value of 0.87 which was considered to be reliable. Five hundred and twenty-one (521) copies of questionnaire were administered, and 470 copies retrieved; and were used for data analysis. Mean and standard deviation were used in analysing research questions and t-test statistics for testing the null hypotheses at 0.05 level of significance.

Findings of the Study

Research Question One: What are the intelligent strategies applicable in managing cybersecurity?

Table 1: Mean Ratings and Standard Deviations on Intelligent Strategies Applicable in Managing Cybersecurity (N = 470)

S/N	Intelligent Strategies Applicable in Managing Cybersecurity	($\bar{x}$)	SD	Decision
1	Updating the system regularly for defending against cyber-attacks	3.42	0.68	Agree
2	Being smart in changing passwords	3.56	0.61	Agree
3	Understanding best practices in data sharing	3.39	0.72	Agree
4	Increased level of phishing awareness	3.47	0.65	Agree
5	Using root cause analysis to identify the source of a security breach	3.28	0.77	Agree
6	Having passion for learning to be transformed from passive to active on duty	3.31	0.74	Agree
7	Facilitating effective communication	3.24	0.79	Agree
8	Collaborating with others in times of risks	3.36	0.71	Agree
9	Possessing a strong sense of cybersecurity awareness	3.63	0.58	Agree
10	Tactically developing effective solutions to cybersecurity challenges	3.41	0.69	Agree
11	Possessing basic incident response skills	3.26	0.75	Agree
12	Possessing a strong foundation in business principles combined with cybersecurity knowledge	3.33	0.73	Agree
13	Utilizing threat intelligence data to inform risk management practices	3.22	0.81	Agree
14	Possessing security skills applicable to the use of public cloud platforms	3.18	0.83	Agree
Grand Mean		**3.36**	**0.72**	**Agree**

Researcher's field work, 2026

Table 1 shows the mean ratings and standard deviations of respondents on the intelligent strategies applicable in managing cybersecurity. The results reveals that all the listed strategies had mean scores above the criterion mean of 2.50, showing agreement among respondents that they are applicable intelligent strategies for managing cybersecurity. The highest-rated strategy was possessing a strong sense of cybersecurity awareness ($\bar{x}$ = 3.63, SD = 0.58), followed by being smart in changing passwords ($\bar{x}$ = 3.56, SD = 0.61). The least-rated strategy, though still agreed upon, was possessing security skills applicable to the use of public cloud platforms ($\bar{x}$ = 3.18, SD = 0.83). The grand mean of 3.36 shows overall agreement that the identified strategies are applicable in managing cybersecurity. The standard deviation values, ranging from 0.58 to 0.83, suggest a relatively close agreement among respondents.

Research Question Two: What are the abilities of business education students in applying intelligent strategies to managing cybersecurity?

Table 2: Mean Ratings and Standard Deviations on the Abilities of Business Education Students in Applying Intelligent Strategies to Managing Cybersecurity (N = 470)

S/N	Abilities of Business Education Students in Applying Intelligent Strategies	($\bar{x}$)	SD	Decision
15	Ability in manipulating cybersecurity tools	3.21	0.79	Agree
16	Demonstrating business skills	3.27	0.74	Agree
17	Using network security monitoring tools to monitor threats	3.18	0.82	Agree
18	Using strategic threat assessment	3.15	0.85	Agree
19	Using risk management practices	3.24	0.77	Agree
20	Familiarity with operating systems	3.34	0.71	Agree
21	Being knowledgeable in incident response	3.17	0.83	Agree
22	Being conversant in using effective communication	3.42	0.67	Agree
23	Strong desire for continuous learning	3.51	0.62	Agree
24	Collaborative attitude at work	3.47	0.64	Agree
25	Adaptability in various situations	3.39	0.69	Agree
26	Being able to think strategically	3.36	0.71	Agree
27	Using antivirus software to block computer viruses from infecting devices	3.45	0.66	Agree
28	Using intrusion detection to detect threats	3.12	0.86	Agree
29	Using penetration testing measures	3.08	0.89	Agree
30	Using vulnerability scanners to find vulnerabilities in systems	3.11	0.87	Agree
31	Using firewalls to filter malicious traffic from entering networks	3.29	0.73	Agree
Grand Mean		**3.28**	**0.76**	**Agree**

Researcher's field work, 2026

Table 2 presents the mean ratings and standard deviations on the abilities of business education students in applying intelligent strategies to managing cybersecurity. The findings reveal that all the identified abilities recorded mean scores above the criterion mean of 2.50, indicating agreement among respondents that these abilities are necessary for the effective application of intelligent cybersecurity strategies. The highest-rated ability was having a strong desire for continuous learning ($\bar{x}$ = 3.51, SD = 0.62), followed by a collaborative attitude at work ($\bar{x}$ = 3.47, SD = 0.64) and the ability to use antivirus software ($\bar{x}$ = 3.45, SD = 0.66). The least-rated ability was using penetration testing measures ($\bar{x}$ = 3.08, SD = 0.89), though respondents still agreed that it is important. The grand mean of 3.28 shows overall agreement that business education students possess the identified abilities needed to apply intelligent strategies in managing cybersecurity. The standard deviation values indicate a relatively low dispersion in respondents' opinions.

Hypothesis 1**:** There is no significant difference in the opinions of students from federal and state tertiary institutions on the intelligent strategies applicable in managing cybersecurity.

Table 3: Independent Samples t-Test on Mean Ratings of Federal and State Tertiary Institution Students on Intelligent Strategies Applicable in Managing Cybersecurity (N = 470)

Institution Type	N	x̄	SD	df	t-cal	t-crit	Decision
Federal	382	3.37	0.41				
State	88	3.34	0.44	468	0.62	1.96	Not Significant
Total	470						

Table 3 shows that federal institution students had a mean rating of 3.37 (SD = 0.41), while state institution students had a mean rating of 3.34 (SD = 0.44) on the intelligent strategies applicable in managing cybersecurity. The calculated t-value of 0.62 is less than the critical t-value of 1.96 at 468 degrees of freedom and 0.05 level of significance. Therefore, the null hypothesis was not rejected. This implies that there is no significant difference in the opinions of students from federal and those of state tertiary institutions regarding the intelligent strategies applicable in managing cybersecurity.

Hypothesis 2: There is no significant difference in the opinions of students from federal and state tertiary institutions on the abilities of business education students in applying intelligent strategies to managing cybersecurity.

Table 4: Independent Samples t-Test on Mean Ratings of Federal and State Tertiary Institution Students on the Abilities of Business Education Students in Applying Intelligent Strategies to Managing Cybersecurity (N = 470)

Institution Type	N	x̄	SD	df	t-cal	t-crit	Decision
Federal	382	3.30	0.46				
State	88	3.25	0.48	468	0.90	1.96	Not Significant
Total	470						

Table 4 shows that students from federal institution recorded a mean rating of 3.30 (SD = 0.46), whereas those of state institutions recorded a mean rating of 3.25 (SD = 0.48) on the abilities of business education students in applying intelligent strategies to managing cybersecurity. The calculated t-value of 0.90 is less than the critical t-value of 1.96 at 468 degrees of freedom and 0.05 level of significance. Consequently, the null hypothesis was not rejected. This means that there is no significant difference in the opinions of students from federal and those of state tertiary institutions concerning the abilities of business education students in applying intelligent strategies to managing cybersecurity.

Discussion of Findings

The findings from Table one revealed that business education students agreed that several intelligent strategies are applicable in managing cybersecurity. These strategies include regular system updates, intelligent password management, phishing awareness, continuous learning, threat intelligence utilization, incident response skills, cybersecurity awareness, collaboration, effective communication, cloud security competence, and the integration of business and cybersecurity knowledge. The high grand mean obtained indicates strong consensus among respondents regarding the relevance of these strategies. The finding that regular system updates are essential for cybersecurity management supports Adamu et al. (2020), who emphasized that software updates and patch management reduce vulnerabilities and protect systems from emerging cyber threats. Similarly, the importance attached to password management and phishing awareness aligns with Payne et al. (2020) and Oyefeso and Abdulkareem (2025), who reported that strong password practices and cybersecurity awareness training significantly reduce the likelihood of successful cyber-attacks.

The corresponding hypothesis in Table 3 indicated that there was no statistically significant difference between the opinions of students from Federal and State tertiary institutions regarding intelligent strategies applicable in managing cybersecurity. The calculated t-value of 0.62 is less than the critical t-value of 1.96 at 468 degrees of freedom and 0.05 level of significance. Therefore, the null hypothesis was not rejected. This suggests that regardless of institutional ownership, students possess similar perceptions concerning intelligent strategies applicable in managing cybersecurity.

The study also revealed threat intelligence utilization and root cause analysis as important cybersecurity strategies. This finding agrees with Obiakor et al. (2025), who noted that cyber threat intelligence enables individuals and organizations to identify vulnerabilities, anticipate attacks, and strengthen security resilience. Likewise, the finding on continuous learning corroborates Oyefeso and Abdulkareem (2025), who argued that the dynamic nature of cyber threats requires constant updating of knowledge and skills. The recognition of collaboration, communication, and cybersecurity awareness further support Obiakor et al. (2025), who maintained that cybersecurity management, requires both technical expertise and collective organizational effort.

Furthermore, Table 2 revealed that the students possess several abilities necessary for applying intelligent cybersecurity strategies. These abilities include the use of cybersecurity tools, network monitoring, strategic threat assessment, risk management, incident response, communication, collaboration, adaptability, and strategic thinking. Students were also perceived to possess competencies in the use of cybersecurity technologies such as antivirus software, intrusion detection systems, vulnerability scanners, penetration testing tools, and firewalls. The finding that students can utilize cybersecurity tools and technologies supports Osijirin et al.

(2025), who reported that digital competence and technological proficiency are increasingly important among university students. Similarly, the finding on strategic thinking and risk management also agrees with Osijirin et al. (2025), who emphasized that effective cybersecurity management requires proactive decision-making, risk evaluation, and preventive action. The result also reinforces the interdisciplinary nature of cybersecurity, which combines business knowledge with technological competence.

The corresponding hypothesis in Table 4 revealed no significant difference in the opinions of students from federal and those of state tertiary institutions concerning the abilities of business education students in applying intelligent strategies to managing cybersecurity. Hence, the null hypothesis was not rejected. The study further revealed that students possess adaptability, collaborative skills, and a willingness to engage in continuous learning. This finding is consistent with the position of the World Economic Forum, which identified adaptability, lifelong learning, teamwork, and problem-solving as critical competencies in the digital age. In addition, the importance attached to practical experience with cybersecurity technologies agrees with Garba et al. (2020), who emphasized that hands-on experience with security tools enhances cybersecurity competence and preparedness for addressing cyber threats.

Overall, the findings suggest that business education students recognize the importance of intelligent cybersecurity strategies and possess many of the competencies required for effective cybersecurity management. However, sustained training, practical exposure, and continuous skill development remain necessary to strengthen their capacity to respond to evolving cyber threats.

Conclusion

Based on the findings of the study, it was concluded that business education students require a broad range of intelligent strategies to effectively manage cybersecurity challenges in contemporary digital environments. The study established that cybersecurity management extends beyond technical expertise to include strategic thinking, continuous learning, effective communication, collaboration, cybersecurity awareness, risk assessment, and incident response capabilities. The findings further revealed that business education students possess various abilities that can support the application of these intelligent strategies, including the use of cybersecurity tools, business skills, adaptability, strategic decision-making, and the ability to utilize security technologies.

The increasing digitization of business operations and educational activities has made cybersecurity competence an essential requirement for business education students. Therefore, equipping students with relevant intelligence strategies and practical cybersecurity skills will enhance their ability to identify, prevent, and respond to cyber threats while contributing effectively to organizational security and business continuity. Consequently, the integration of cybersecurity intelligence strategies into business

education programmes is necessary for producing graduates who can function effectively in today's technology-driven business environment.

Recommendations

Based on the findings of the study, the following recommendations were made:

1. Tertiary institutions should provide students with access to cybersecurity laboratories and simulation environments where they can gain practical experience using cybersecurity tools and technologies.
2. Tertiary institutions should collaborate with cybersecurity professionals, organizations, and industry stakeholders to expose students to current cybersecurity trends, best practices, and emerging threats.

REFERENCES

Adamu, A. G.; Sirat, M. B.; Hajar, S.; Dauda, I. B. (2020). Cyber 'security awareness among university students: A case study: *Science Proceedings Series* 2(1)

Admins, M. (2024). 17 essentials skills for cybersecurity success,Marymount.edu

Aliyu, A., Aliyu, A., Ahmad, A. & Abdullahi, S. (2021). Investigation of cybersecurity awareness among tertiary institutions in Nigeria. *International Journal of Advances in Engineering and Measurement (IJAEM) 3*(10), 111-118. www.ijaem.net

Azad, R. U., Tasmin, S. & Atikuzzaman (2025). Investigating students' awareness of online privacy and cybersecurity: An empirical study with effective cybersecurity training framework. *Global Knowledge Memory and Communication*. DIO: 10.1108/KGMC-05-2024-0319

Garba, A. A., Siraj, M. M.; Othman, S. H. & Musa, M. A. (2020). A study on cybersecurity awareness among students in Yobe State University, Nigeria: A quantitative approach. *International Journal of on Emerging Technologies 11(5): 41-49*

Garba, A. A., Sirat, M. B., Otheman, S. H, & Dauda, I. B. (2020). Cyber security awareness among university students: A case study. *Science Proceedings Series 2*(1), 82-86, researchgate.net.

Graham, S (2025). Essentials cybersecurity skills for security analysts in 2026. Courser.org;

Khalid, F., Daud, M. Y., Rahman, M. J. & Nasir, K. M. (2018). An investigation of university students' awareness on cyber security. *International of Engineering & Technology: 7*(21), 11-14

Khan, K. (2024). Overview of security intelligence. Linkelin.com

Lindemulder, G. and Kosinki, M. (2024). What is Cyber security? www.ibm.com

Obiakor, I. N.; Onyesolu, M. O.; & Julius, M. S. (2025). Cyber threat intelligence sharing: A strategic tool for enhancing national and global security postures. *World Journal of Advanced Engineering Technology and Science Journal, 17*(02), 444-453 https://wjaets.com/

Ogene, F. (2024). Cybersecurity and IT Governance Challenges in Nigeria: Strategies Investment Needs and the Path Forward for a Resilient Digital Economy. *International Journal of Computer Application, (075 – 8887). 186 (55).* Ijcaonline.org

Edeh, M. O. (2021). Cybersecurity Awareness among Undergraduate Students in Enugu, Nigeria: *International Journal of Information and Security; Privacy and Digital Forensics (Nigeria Computer Society)*

Osijirin, A. N., Utibe, V. & Mohammed, S. (2025). Impact of awareness of cybersecurity among tertiary institution students in Enugu State, Nigeria. *International Journal of Innovative Science & Technology, 10*(3), researchgate.net

Osijirin, A. N.; Sada, S. M.; Edmond, V. U.; Anigbo, L. C.; & Okechukwu, O. (2026). Cybersecurity awareness and online safety practices among tertiary institution students in Enugu State: *International Journal of Computer Science and Mathematical Theory (IJCSMT)* www.ijardjounrals.org

Oyefeso, O. O. & Abdulkareem, S. (2025). Role of cybersecurity awareness in safeguarding digital systems in institutions of higher learning. Kontagora *Journal of Intellectual Discourse (KJID), 3(1)*

Payne, B. K.; Cross, B.; & Vandecar-Burdin, T. (2022). Faculty and advisor advice for cybersecurity students: Liberal arts, interdisciplinary, experience, lifelong learning, technical skills, and hard work. *Journal of Cybersecurity Education, Research and Practice. https://files.eric.ed.gov/fulltext/EJ1332788.pdf*

Sternberg, R. J. (n.d.). Encyclopaedia Britannica

Sule, et al Sule, B.; Yahaya, M. A.; Sambo, U.; & Mat, B. (2021). Cybersecurity and cybercrime in Nigeria: The implications on

national security and digital economy. *Journal of Intelligence and Cyber Security*. www.researchgate.net

Wadhwa, P. (2026). Security Intelligence – What is the role of intelligence in security. Sprito.com

Wiechetek, L & Medrek, M. (2023). Human factors in Security – Cybersecurity education and awareness of business students. *Annales Universitatis Mariae Curie-Sklodowska,section H – Oeconomia, 56(1)*

World Economic Forum Global Risks Report (2024). Global Risks Report 2024. www.weforum.org