AMERICAN JOURNAL OF
BUSINESS AND MANAGEMENT INNOVATION (AJBMI)

VOLUME 1 ISSUE 1 (2026)



PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Business and Management Innovation (AJBMI)

Volume 1 Issue 1, Year 2026
ISSN: 3143-4576 (Online)
DOI: https://doi.org/10.54536/ajbmi.v1i1.9059
https://journals.e-palli.com/home/index.php/ajbmi

Cybersecurity Awareness and Data Privacy: A Comparative Study of Administrative Staff in Federal and State Tertiary Institutions in Akwa Ibom State, Nigeria

Effiong Effiong Ebieme[1*], Comfort Idongesit Charles[1], Anietie Bello Inyang[2]

Article Information

Received: August 22, 2026

Accepted: November 09, 2026

Published: November 13, 2026

Keywords

Administrative Staff, Business Education, Cybersecurity Awareness, Data Privacy, Nigeria Data Protection Act (NDPA)

ABSTRACT

This study examined cybersecurity awareness and data privacy: A comparative study of administrative staff in federal and state tertiary institutions in Akwa Ibom State, Nigeria. It was driven by the enforcement of the Nigeria Data Protection Act (NDPA) and rising digital vulnerabilities in higher institutions. The study adopted a comparative descriptive survey research design. A non-probability purposive sampling technique was utilized to select 200 administrative professionals across four institutions, representing a balanced 2 x 2 multi-tier structure. Data collection was executed via "Cybersecurity Awareness and Data Privacy Questionnaire (CADPQ)", validated by three experts and obtained Cronbach's alpha reliability coefficient of 0.86. Mean and standard deviation were used to answer research questions, while the independent samples t-test was used to test the null hypotheses at .05 level of significance. The findings of the study revealed that administrative staff in federal tertiary institutions have greater cybersecurity awareness and data privacy compliance than their state counterparts. The study concluded that these significant disparities persist largely due to unequal access to funding, digital infrastructure and structured training. It was recommended, among others, that the Management of state tertiary institutions should set up regular, mandatory training and workshops for administrative staff to close up the cybersecurity awareness and data privacy compliance gap. These research outcomes reveal an urgent need to review the Business Education curriculum, transforming it to systematically integrate advanced data ethics, regulatory compliance frameworks, and proactive digital security competencies essential for modern workplace.

INTRODUCTION

Technology has completely changed how universities run today. Instead of piles of physical files, academic institutions now manage massive amounts of digital information, including student records, grades, staff payroll, and research data (Brooks & McCormack, 2020; Vial, 2019). This shift makes universities prime targets for hackers and cybercriminals. Interestingly, the biggest security risk usually is not the software of the computers themselves, it is the human element (Salam *et al.,* 2026). The administrative staff who handle these systems every single day serve as the frontline of defense, meaning their daily habits can either protect or compromise an entire institution (Chikwendu & Oli, 2023).

In Nigeria, this issue is no longer just a technical concern, it is a major legal requirement, with the passage of the Nigeria Data Protection Act (NAPA), public institutions are legally required to protect personal data from unauthorised access. For those of us training future office professionals in Business Education, this reality changes everything. We can no longer just teach basic clerical skills or simple typing (Ebieme & Daniel, 2026). We have to prepare students to navigate data laws and protect sensitive business information in a highly digital work environment (Heinrich & Gerhart, 2023; Irish *et al.*, 2025).

However, there is often a noticeable difference in how different types of institutions handle these changes. Federal Universities, like the University of Uyo (UNIUYO) and the Federal University of Technology, Ikot Abasi (FUTIA), usually have better access to direct national funding, uniform digital tools, and centralised training programmes. On the other hand, State-funded institutions, such as Akwa Ibom State University (AKSU) and Akwa Ibom State Polytechnic (AKWAPOLY) rely on state budgets and local guidelines, which can lead to differences in funding and training. This raises an important question: Do administrative staff in federal and state tertiary institutions have the same level of security awareness and data privacy habits?

While there is plenty of research on IT networks and firewalls, very few studies actually look at the behaviours and skills of the administrative staff running these offices, especially in a developing region like Akwa Ibom State. This is exactly where this study comes in. By comparing the cybersecurity awareness and data privacy habits of federal and state institutional workers, this paper bridges a significant gap in our field. Most importantly it provides the solid data needed to update Business Education curriculum, ensuring graduates are ready for the security challenges of the modern workplace.

Statement of the Problem

The core problem addressing this study is the high

[1] Department of Business Education, University of Uyo, Uyo, Nigeria
[2] Department of Business Education, Akwa Ibom State University of Education, Afaha Nsit, Nigeria
[*] Corresponding author's e-mail: effiongbieme7@gmail.com

vulnerability of public tertiary institutions in Akwa Ibom State to data breaches, driven largely by suboptimal cybersecurity habits among administrative staff. With the enforcement of the Nigeria Data Protection Act (NDPA, 2023s; 2024} institutions are under strict legal pressure to safeguard sensitive academic, financial and personal data. Despite these mandates many administrative staff, who serve as the daily gatekeepers of institutional databases still struggle with basic security protocols, such as recognising phishing emails, maintaining proper password hygiene, and handling records securely. This lack of practical security awareness creates a weak link in university administration, leaving schools exposed to insider errors, identity theft, and severe regulatory penalties.

This problem is further complicated by systemic funding and training disparities between federal and state-owned tertiary institutions like the University of Uyo (UNIUYO) and Federal University of Technology, Ikot Abasi (FUTIA) often have better access to centralized tech funding and structured data-governance training, state institutions like Akwa Ibom State University (AKSU) and Akwa Ibom State Polytechnic (AKWAPOLY) frequently face fighter fiscal limits. These unequal realities suggest that state administrative staff may be significantly less prepared to handle digital threats than their federal counterparts, leading to an uneven security landscape across the state. If these behavioural and institutional gaps are left unaddressed, tertiary institutions will remain highly vulnerable to cyber risks, and Business Education curriculum will continue to turn out graduates who lack the modern, security-conscious administrative skills required by today's digital workforce. Therefore, this study seeks to fill the gap identified in the literature by investigating cybersecurity awareness and data privacy: A comparative study of federal and state tertiary institutions in Akwa Ibom State, Nigeria.

Objectives of the Study

The primary objective of this study is to investigate cybersecurity awareness and data privacy: A comparative study of administrative staff in federal and state tertiary institutions in Akwa Ibom State, Nigeria. Specifically, the study sought to:

1. Assess the difference in cybersecurity awareness between administrative staff in federal and state tertiary institutions in Akwa Ibom State, Nigeria.
2. Determine the difference in data privacy compliance behaviour between administrative staff in federal and state tertiary institutions in Akwa Ibom State, Nigeria.

Research Questions

What is the difference in cybersecurity awareness between administrative staff in federal and state tertiary institutions in Akwa Ibom State, Nigeria.

What is the difference in data privacy compliance behavior between administrative staff in federal and state tertiary institutions in Akwa Ibom State, Nigeria.

Research Hypotheses

H01: There is no significant difference in cybersecurity awareness between administrative staff in federal and state tertiary institutions in Akwa Ibom State, Nigeria.

H02: There is no significant difference in data privacy compliance behaviour between administrative staff in federal and state tertiary institutions in Akwa Ibom State, Nigeria.

LITERATURE REVIEW

Concept of Cybersecurity Awareness

Scholars look at cybersecurity awareness from multiple angles. While institutional frameworks view it as a corporate training process researchers focus on it as an individual mix of knowledge, choices and habits. According to Kruger & Kearney (2006) cybersecurity awareness is an individual's combined understanding, attitude, and actual workplace behaviours regarding the active preservation of corporate data assets. Bulgurcu *et al.* (2010) characterised it as an employee's comprehensive baseline knowledge of system safety rules, which directly drives their intent to follow protective guidelines. It is described as the depth of technology user's cognitive understanding of digital risks and their personal responsibility to preserve network protections (Shaw *et al.*, 2009). It is also viewed as an ongoing educational process where system users remain mindful of organisational safety boundaries and apply those rules to their everyday computer habits (Siponen, 2000). D'Arcy *et al.* (2009) characterised it as an employee's conscious internal alignment with visible security cues, policy reminders, and formal institutional security education.

Albrechsten (2007) identified it as a shared cultural practice within a workplace where personnel hold uniform interpretations of digital threats and co-ordinate their actions to prevent them. It is described as the measurable combination of knowledge, safety attitudes, and practical behaviours exhibited by staff during daily computing tasks (Parsons *et al.,* 2014). McCormac *et al.* (2017) defined it as the practical manifestation of a worker's personal information security knowledge, which dictates how safely they process files online. It is an office professional's conscious attention to data controls, serving as the primary barrier against accidental information leaks (Liginlal *et al.,* 2009). It is also viewed as a structured psychological shift where passive computer operators develop proactive, defensive habits against social engineering schemes (Bada *et al.,* 2015). Abawajy (2014) described it as the ultimate combination of risk comprehension and manual skill required of a user to successfully neutralize malicious emails and hacking attempts. It is an ordinary employee's clarity regarding everyday computer protection, allowing them to easily spot fraudulent traps in their workspace (Furnell *et al.,* 2007). It is also the critical cognitive balance between a worker's daily workload stress, their technical carelessness, and their compliance with information safety protocols.

Data Privacy

Understanding how information privacy shifts between individual rights and institutional responsibilities is critical for data governance. Westin (1967) described data privacy as the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. It is viewed as a dynamic interpersonal boundary-control process that allows individuals to regulate their social interactions and dictate what information is accessible to the public (Altman, 1975). It is also viewed as "information privacy" which is the interest an individual has in sustaining a personal space, free from interference, regarding the collection and handling of their digital footprints (Clarke & Chalmers, 1988). It can further be viewed as a control-based psychological state where individuals can selectively limit or grant access to their personal history, choices, and identifying characteristics.

According to Solove (2006) data privacy is not a single concept, but as a cluster of distinct activities including information collection, processing, dissemination, and invasion that must be legally regulated. It is described as an organisation's structural commitment to fairness, transparency and accountability when processing personal customer or employee data (Culnan & Bies, 2003). It can also be described as an individual's specific concerns regarding organizational practices, specifically focusing on the unauthorized collection, improper access, secondary use, and errors in personal files (Smith *et al.*, 1996).

Data privacy can be viewed as a systemic capability where an institution aligns its information processing behaviours with the explicit privacy expectations of its stakeholders (Greenaway *et al.* 2015). It is viewed as the engineering and administrative practice of minimising personal data exposure within software systems, ensuring compliance with global regulatory baselines (Spiekerman & Cranor, 2009). It is also viewed as a public administrator's professional adherence to institutional security protocols, preventing insider threats from compromising third-party registries (Ebieme & Umana, 2026). It could further be viewed as a measurable state of regulatory compliance where organisations systematically implement technical privacy features (like explicit consent mechanisms) to satisfy regional data protection mandates. Simply put, it is a "contextual integrity" which requires that personal information flows must strictly adhere to the established norms and expectations of a specific social or professional setting.

Global Trajectories in Data Privacy Policy

On the international stage, data privacy policies have transitioned from loose organisational guidelines into aggressive, legal binding frameworks designed to govern the modern digital footprint. The foundational blueprint for global compliance is anchored by the European Union's General Data Protection Regulation (GDPR), which established data protection as a fundamental human right rather than a mere consumer choice. The GDPR fundamentally transformed administrative operations worldwide by introducing the principles of accountability, data minimisation, and "privacy by design", while imposing severe financial penalties for institutional negligence. Similarly, frameworks like the California Consumer Privacy Act (CCPA) in the United States and the Asia-Pacific Economic Co-operation (APEC). Privacy framework have forced public and private entities to overhaul their information storage systems. In higher education administration globally, these policies mean that student records, medical entries and institutional databases can no longer be handled casually; they require strict access controls, transparent consent mechanisms, and clear pathways for data erasure.

The Nigerian Data Governance Landscape: The NDPA Framework

Domestically, Nigeria's regulatory stance on data governance reached a historical milestone with the enactment of the Nigeria Data Protection Act (NDPA), which established the Nigeria Data Protection Commission (NDPC) as the apex regulatory authority. Moving past the initial, fragmented guidelines of the 2019 National Information Technology Development Agency (NITDA) rules, the NDPA serves as a comprehensive statutory framework that legally obligates all institutional data controllers and processors to protect personal information. For public tertiary institutions in Nigeria, the implications are immediate and profound. Academic registries, bursary departments, and administrative offices are legally responsible for safeguarding massive tranches of student and personnel data from unauthorised exposure or insider leaks. Under the NDPA, statutory compliance is no longer a bureaucratic option; institutional administrators are held personally and structurally accountable for data handling errors, making comprehensive security awareness a critical operational necessity within public administration.

Administrative Staff

Administrative personnel in tertiary settings serve as data custodians. Blau & Scoff (1962) described them as the functional core of an organisation responsible for coordination, communication, and maintaining continuity across different units. They are the "support staff" and the "technostructure" who provide vital internal services outside the mainstream operational flow (Mintzberg, 1979). Simon (1997) characterised them as the decision-enabling agents who process information, manage records, and establish the communication lines that allow executives to lead. They are the maintenance subsystem of an organisation, responsible for keeping the physical and digital infrastructure stable (Katz & Kahn, 1978). Drucker (1999) characterised them as knowledge workers tasked with translating executive strategic policies into daily operational routines.

According to Altbach (2005) administrative staff are the

"third force" in higher education, distinct students and faculty who manage the complex operations of modern universities. Gornitzka & Larsen (2004) characterised them as institutional professionals whose duties have shifted from simple clerical typing to specialised data and resource management. Rhoades (1998) described them as "managed professionals" who control institutional resources, student admissions, examinations, and payroll systems. They are the "boundary spanners" in higher education who work across academic, technological, and corporate domains (Whitchurch (2008). Szekeres (2011) described them as the invisible workers of the university who keep the institution running smoothly while adapting to global performance metrics. They are the organisational backbone whose digital literacy and statistical capability directly influence the administrative productivity of an organisation (Ebieme, 2026; Ebieme *et al.*, 2026). They can also be described as executive office professionals trained to manage modern office information systems while, maintaining digital records compliance (Enyetip & Ebieme, 2026; Ebieme & Bassey, 2026).

Theoretical Framework

This study is anchored on two complementary behavioural models: Protection Motivation Theory (PMT) and Technology Threat Avoidance Theory (TTAT). Together, these theories explain, the cognitive and behavioural factors that drive or hinder cybersecurity awareness and data privacy compliance behaviour between administrative staff in federal and state tertiary institutions in Akwa Ibom State, Nigeria.

Protection Motivation Theory – Ronald W. Rogers (1975)

Protection motivation theory, originally developed by Rogers (1975) and expanded in 1983, posits that individuals adopt protective behaviours based on a cognitive evaluation process balancing two main channels: threat appraisal and coping appraisal.

- Threat appraisal: this involves an individual's evaluation of the seriousness of a threat (perceived severity) and their likelihood of being affected by it (perceived vulnerability). In this study, an administrative staff member evaluates how damaging a university database breach would be and how vulnerable their specific registry is to digital attacks.
- Coping appraisal: this focuses on an individual's evaluation of the protective response. It includes response efficacy (the belief that security habits like complex passwords, will actually block a hacker) and self-efficacy (the individual's personal confidence in their ability to execute these protocols correctly).

PMT is highly relevant to this study's comparative design

- It provides a structured framework to evaluate whether differences in funding, infrastructure, and access to regular technology workshops give federal administrative staff (UNIUYO & FUTIA) higher self-efficacy and response efficacy than state-tier staff (at AKSU & AKWAPOLY). If state-tier administrative workers feel less trained, their coping appraisal drops, leading to lower protection motivation and weaker data privacy habits.

Technology Threat Avoidance Theory – Huigang Liang & Yajiong Xue (2009)

While PMT provides a broad foundation for protective actions, the Technology Threat Avoidance Theory, formulated by Liang & Xue (2009) focuses specifically on how human users behave in the presence of digital IT threats. TTAT states that a user's motivation to avoid a technology threat (such as an accidental data leak or a malware infection) depends on their perception of the threat, the perceived costs of avoiding it, and their specific tech skills.

A critical element of TTAT is the balance between avoidance costs and threat motivation. In a busy higher education registry, administrative staff handle large volumes of student transcripts, financial statements, and personnel files daily. If workers feel that strict data privacy rules (like multi-factor authentication, encryption, or detailed access logs) create a high avoidance cost by making their regular duties too slow or tedious, TTAT predicts they will bypass security protocols to save time. Furthermore, TTAT links threat avoidance directly to technical competency. This model supports the core argument of this study: to lower institutional insider risks under the Nigeria Data Protection Act (NDPA), the university should improve the hands-on technical skills of the workforce. This directly highlights the urgent need to review the Business Education curriculum, transforming it to build a real-world threat avoidance skills and practical compliance training into future office managers before they step into the public sector workforce.

Empirical Framework

Oyefeso & Saleh (2025) investigated the role of cybersecurity awareness in safeguarding digital systems within institutions of higher learning in the North Central region of Nigeria. A descriptive survey design was employed to address three research questions focusing on awareness levels, prevalent threats, and strategies for improvement. The study sampled 168 participants including students, lecturers and administrators from the Federal University of Education, Kontagora and Abdullahi Kure University, Minna. Data were collected using a structured, expert-validated questionnaire with strong internal consistency (Cronbach's alpha = 0.82), and analysed through descriptive awareness across groups, with phishing, malware and data breaches being the most common threats. This work relates to the present study because, it considered the independent variables used in the present study, although the respondents, institutions and geographical location differs.

Ugo-Onyeka *et al.* (2026) examined cybersecurity

readiness and data protection practices in Nigerian tertiary institutions. Drawing from empirical and review-based studies, the discussion identified critical dimensions: Policy framework, cybersecurity infrastructure, awareness and training access control and data protection mechanisms, incident response systems, and institutional governance. Evidence shows that while some institutions have begun implementing basic cybersecurity measures, significant gaps persist in policy enforcement, infrastructure development, and user awareness. This work relates to the present study because it was carried out in higher institutions just like the present study, although different participants were used.

Dabai & Ibrahim (2026) carried out a comparative study on awareness and application of cybersecurity practices between federal and state tertiary institutions in Kebbi State, Nigeria. A structured questionnaire was distributed to 225 respondents (students, lecturers and administrators) across nine institutions, three federal and six state, gathering data on cybersecurity awareness, extent of practice application, institutional support and the challenges hindering adoption. Data were analysed using the Statistical Package for Social Sciences (SPSS), employing simple frequency counts and a 4-point Likert scale to answer the descriptive research questions and using an independent sample t-test to test the two null hypotheses. Results show that respondents in federal institutions reportedly marked higher awareness of phishing, malware and data-protection threats than their state counterparts and applied core cybersecurity practices such as password hygiene, two-factor authentication, software updates and data backup to a significantly greater extent. Federal institutions were also better supported with cybersecurity training, firewalls and documented security policies, while state institutions reported funding constraints, limited technical staff and low security culture as major barriers. This work is relevant to the present study because, it covered the independent variable used in the present study and was also a comparative study. However, the participants used and geographical locations significantly differs.

The review of the empirical works on cybersecurity awareness and data privacy reveals that studies were carried out on various angles of cybersecurity, but not solely focused on administrative staff, who are the engine rooms of both public and private organisations. Therefore, this present study sought to fill the gap identified in the literature by investigating cybersecurity awareness and data privacy: A comparative study of administrative staff in federal and state tertiary institutions in Akwa Ibom State, Nigeria.

MATERIALS AND METHODS

Research Design

This study adopted a comparative descriptive survey research design. This design is uniquely suited for systematically observing, documenting, and comparing the baseline levels of cybersecurity awareness and data privacy compliance behaviour between administrative staff in federal and state tertiary institutions as they occur without manipulating the variables under study (Creswell & Creswell, 2018; Ebieme *et al.,* 2026; Nworgu, 2015). The study was conducted in Akwa Ibom State Nigeria, a major educational, economic and industrial hub in the Niger Delta region of Nigeria, which hosts premium federal and state tertiary institutions.

Population of the Study

The population for this study comprised all administrative staff in the four selected federal and state tertiary institutions in Akwa Ibom State, Nigeria. The target population specifically focused on administrative personnel deployed in data-sensitive registries, units and departments (such as Admission, Examinations and Records, Human Resources/Establishment, and Accounts/Bursary) within four selected public tertiary institutions. These four specific institutions were deliberately selected over other public or private options in the state to satisfy strict methodological controls:

- Federal Tier: University of Uyo (UNIUYO} and the Federal University of Technology, Ikot Abasi (FUTIA).
- State Tier: Akwa Ibom State University (AKSU), Ikot Akpaden, and the Akwa Ibom State Polytechnic (AKWAPOLY), IKot Osurua.

The deliberate selection of these four specific institutions over other options in the State such as Federal Polytechnic, Ukana, or various private universities was guided by two scientific principles:

- **Symmetrical "Sister-Institution" Pairing:** other public options were excluded because they lacked an equivalent, matching counterpart at the opposite government tier. By choosing these four institutions, the study achieved a balanced comparative design. UNIUYO (Federal Conventional) perfectly pairs with AKSU (STATE Conventional), while FUTIA (Federal Technological) perfectly balanced AKWAPOLY (State Technical). This specific grouping ensured that the final analysis compared similar institutional structures across both tiers of public governance.
- **Exclusion of Private Variables and Data Volume Control:** private tertiary institutions operate under independent corporate budgets and private governance models. Since this study focused strictly on public sector administrative efficiency, private institutions were systematically excluded to keep the data clean. Furthermore, compared to smaller localised campuses like the Federal polytechnic, Ukana, these four selected institutions manage the largest databases, student registries, and personnel records in Akwa Ibom State, making their staff the most logistically relevant and legally scrutinised data handlers under the Nigeria Data Protection Act (NDPA).

Sampling Technique and Sample Size

A non-probability purposive sampling technique was employed to select the participants for the study. This

technique was deemed most appropriate because it allowed the researcher to deliberately target respondents who interact directly with institutional data management platforms, student records, and electronic information networks on a daily basis, rather than selecting staff whose duties carry no exposure to data threats.

To total sample size of 200 respondents was utilised for the study. To ensure equal representation and a statistically balanced framework across the institution tiers, a uniform cohort of fifty (50) administrative staff was purposively sampled from each of the four selected institutions, yielding a perfect 100 versus 100 group distribution:

• Federal Tier (N1 = 100): UNIUYO (50 staff) and FUTIA (50 staff)

• State Tier (N¬2 = 100): AKSU (50 staff) and AKWAPOLY (50 staff)

The inclusion criteria strictly restricted the sample to administrative professionals who handle confidential student records, staff payroll, policy documents, or institutional database registries, thereby serving as the primary human firewall for data privacy compliance within their respective institutions.

Instrument, Validity and Reliability

The primary instrument used for data collection was a modified 4-point Likert-scale structured questionnaire titled "Cybersecurity Awareness and Data Privacy Questionnaire (CADPQ)". Scoring of the instrument was as follows: strongly Agree (SA)-4; Agree (A)-3; Disagree (D)-2; and Strongly Disagree (SD)-1; the "undecided" option was deliberately omitted to prevent central tendency bias and fence-sitting by respondents.

The instrument was validated by three experts in Information Technology, Business Education, and Measurement and Evaluation at the University of Uyo, Akwa Ibom State, Nigeria. Reliability was confirmed through a pilot test of ten (10) administrative professionals outside the main study pool, yielding a Cronbach's alpha coefficient of 0.86. This was deemed high enough for the study and was supported by Nunnally & Bernstein (1994) cited in Ebieme *et al.* (2024) who asserted that a reliability coefficient of 0.70 should be accepted particularly at the early stage of the research.

Data Collection

The researcher and three trained research assistants administered the copies of questionnaire to the respondents during official working hours, having obtained permission from respective Heads of Units. This enhanced a high retrieval rate and allowed for clarifications when necessary. Respondents were assured of the confidentiality of their responses and those who did not wish to participate in the study were excused. 191 copies of the questionnaire out of 200 copies administered, representing 95.5% were returned in useable form.

The mean and standard deviation were used to answer research questions 1and 2, while an independent samples t-test was used to test the two null hypotheses at .05 level of significance. A cluster means of 2.50 was used to compare the level of cybersecurity awareness and data privacy between federal and state tertiary institutions, with means scores of 2.50 and above indicating a strong agreement and scores below 2.50 indicating a weak agreement. For the t-tests, the null hypothesis was rejected when $P < .05$ and retained when $P >. 05$.

RESULTS AND DISCUSSION

Research Question One

What is the difference in cybersecurity awareness between administrative staff in federal and state tertiary institutions in Akwa Ibom State, Nigeria?

The result presented in Table 1 reveals that the mean cybersecurity awareness score of 22.53 obtained by administrative staff in federal tertiary institutions was greater than the mean cybersecurity awareness score of 16.93 obtained by administrative staff in state tertiary institutions, with a mean difference of 5.60. This result implies that there is a difference in the mean cybersecurity awareness scores of administrative staff in federal and state tertiary institutions in Akwa Ibom State, Nigeria, in favour of administrative staff in federal tertiary institutions.

Table 1: Mean and standard deviation of the difference in cybersecurity awareness between administrative staff in federal and state tertiary institutions in Akwa Ibom State, Nigeria (N=191)

Administrative staff	N	Mean	SD	Mean Difference
Federal	92	22.53	2.81	5.60
State	99	16.93	2.53	

Research Question Two

What is the difference in data privacy compliance behaviour between administrative staff in federal and state tertiary institutions in Akwa Ibom State, Nigeria?

The result presented in Table 2 reveals that the mean data privacy compliance behaviour score of 21.95 obtained by administrative staff in federal tertiary institutions was greater than the mean data privacy compliance behaviour score of 16.61 obtained by administrative staff in state tertiary institutions, with a mean difference of 5.34. This result implies that there is a difference in the mean data privacy compliance behaviour scores of administrative staff in federal and state tertiary institutions in Akwa Ibom State, Nigeria, in favour of administrative staff in federal tertiary institutions.

Table 2: Mean and standard deviation of the difference in data privacy compliance behaviour between administrative staff in federal and state tertiary institutions in Akwa Ibom State, Nigeria (N=191)

Administrative staff	N	Mean	SD	Mean Difference
Federal	92	21.95	3.22	5.34
State	99	16.61	2.21	

Hypothesis One

There is no significant difference in cybersecurity awareness between administrative staff in federal and state tertiary institutions in Akwa Ibom State, Nigeria

Table 3: Independent t-test analysis of the difference in cybersecurity awareness between administrative staff in federal and state tertiary institutions in Akwa Ibom State, Nigeria (N=191)

Administrative staff	N	Mean	SD	t-value	Sig.	Decision
Federal	92	22.53	2.81	14.51	0.00	Significant
State	99	16.93	2.53			

**Significant at P< .05; df= 189*

The result in Table 3 revealed the t-value of 14.51 and the corresponding probability level of significance of 0.00 alpha at 189 degrees of freedom. This level of significance is less than .05 in which the decision is based. With this result, the null hypothesis was rejected. This implies that there is significant difference in cybersecurity awareness between administrative staff in federal and state tertiary institutions in Akwa Ibom State, Nigeria.

Hypothesis Two

There is no significant difference in data privacy compliance behaviour between administrative staff in federal and state tertiary institutions in Akwa Ibom State, Nigeria

Table 4: Independent t-test analysis of the difference in data privacy compliance behaviour between administrative staff in federal and state tertiary institutions in Akwa Ibom State, Nigeria (N =191)

Administrative staff	N	Mean	SD	t-value	Sig.	Decision
Federal	92	21.95	3.22	13.44	0.00	Significant
State	99	16.61	2.21			

**Significant at P< .05; df= 189*

The result in Table 4 revealed the t-value of 13.44 and the corresponding probability level of significance of 0.00 alpha at 189 degrees of freedom. This level of significance is less than .05 in which the decision is based. With this result, the null hypothesis was rejected. This implies that there is significant difference in data privacy compliance behaviour between administrative staff in federal and state tertiary institutions in Akwa Ibom State, Nigeria.

Findings

The findings of the study showed that:

1. there is significant difference in cybersecurity awareness between administrative staff in federal and state tertiary institutions in Akwa Ibom State, Nigeria
2. there is significant difference in data privacy compliance behaviour between administrative staff in federal and state tertiary institutions in Akwa Ibom State, Nigeria

Discussion of Findings

The first objective of this study was to assess the difference in cybersecurity awareness between administrative staff in federal and state tertiary institutions in Akwa Ibom State, Nigeria. The result of answering research question one, and that of the corresponding hypothesis revealed a statistically significant difference in the mean scores of cybersecurity awareness between administrative staff in the federal tertiary institutions (UNIUYO and FUTIA) and those in state-owned tertiary institutions (AKSU and AKWAPOLY). Consequently, the first null hypothesis was rejected. The descriptive data indicated that while federal administrative personnel demonstrated high-to-moderate proficiency in baseline cybersecurity behaviours such as password hygiene and workstation locking. Their state-tier counterparts exhibited noticeable gaps, particularly in complex threats indicators like identifying advanced spear-phishing templates and understanding hidden system vulnerabilities.

This finding aligns with the structural perspectives of Albrechsten (2007), Parsons *et al.* (2014) and Ugo-Onyeka *et al.* (2014) who noted that information security awareness within an organisation is heavily tied to institutional culture and the presence of ongoing, structured educational interventions. In the context of Akwa Ibom State, the higher baseline awareness observed at the federal level can be attributed to more consistent access to centralised funding, regular technical workshops, and standardized digital tools. When viewed through the lens of Protection Motivation Theory (Rogers, 1975), this variance points to a disparity in Coping Appraisal. Because federal administrators have better access to institutional training, their self-efficacy (personal confidence in handling threats) and response efficacy (belief in the security protocols) are significantly higher. Conversely, state-tier personnel often face tighter budgetary constraints and fewer specialised training options, which lowers their overall motivation to maintain proactive cybersecurity habits. This operational reality mirrors the findings of Oyefeso & Saleh (2025) who argued that digital and data literacy gaps among registry personnel in state institutions directly undermine institutional efficiency and leave local databases exposed to outside threats.

The second objective of the study was to determine the difference in data privacy compliance behaviour between administrative staff in federal and state tertiary institutions in Akwa Ibom State, Nigeria. The result of answering research two and testing of the corresponding hypothesis established a statistically significant variance in data privacy compliance behaviours between federal and state institutional administrative staff, leading to the rejection of the second null hypothesis. The data showed that while federal administrative staff at UNIUYO and FUTIA maintained a more structured approach to data handling, records management, and access control, state-tier administrators frequently reported by passing security measures. This included practices such as sharing login credentials across desks or failing to encrypt sensitive student or payroll documents before electronic transmission. This behavioural gap represents a severe structural risk under the Nigeria Data Protection Act, which legally demands absolute confidentiality, integrity and operational accountability from all public data handlers.

This empirical finding supports the arguments of Liginlal *et al.* (2009) who demonstrated that human error within administrative workflows remains the primary catalyst for severe privacy breaches. Furthermore, it validates the warnings of Edoho *et al.* (2025) who noted that registries in South-South Nigerian universities are highly vulnerable to insider threats due to a general lack of operational familiarity with national data protection laws. This non-compliant behaviour can be thoroughly explained using the TTAT (Liang & Xue, 2009). TTAT states that a user's motivation to follow security rules is highly influenced by avoidance costs. In busy higher education registries, staff are under constant pressure to process large volumes of transcripts, admissions, and payroll tasks manually or with limited digital support. When state administrators encounter rigid privacy guidelines without the proper infrastructure or training to back them up, they perceive the security measures as a chore that slows down their workflow. To save tune, they choose to bypass the rules, sacrificing institutional security for operational speed.

Ultimately, these combined deficiencies emphasize the core conclusion of this study: turning out office professionals who lack data ethics and risk awareness creates an immediate vulnerability in our workforce. To build a robust human firewall, there is a clear and urgent need to fundamentally review the Business Education, integrating hands-on cybersecurity literacy, digital threat avoidance, and active compliance training and AI directly into the curriculum before graduates ever enter the modern public sector (Charles & Etuk, 2016; Bassey & Ebieme, 2026; Ukoima *et al.*, 2025; Ebieme & Enyetip, 2026).

CONCLUSION

Based on the findings of the study, it was concluded that significant disparities in cybersecurity awareness and data privacy compliance persist between federal and state tertiary institutions administrative staff in Akwa Ibom State, largely driven by unequal access to funding, digital infrastructure, and structured training. Based on the findings and conclusion of the study, the following recommendations are made:

Organise regular cybersecurity training for state tertiary institutions: since the study revealed that administrative staff in state tertiary institutions (AKSU and AKWAPOLY) have lower security awareness than federal staff [UNIUYO & FUTIA}, Management of state tertiary institutions should set up regular, mandatory training and workshops.

Set clear data rules and update the Business Education curriculum: to fix the differences in how staff handle private records, tertiary institutions in the state should install simple security tools like two-step login verification and encrypted file sharing to prevent accidental data leaks under the Nigeria Data Protection Act (NDPA). Most importantly, the Department of Business Education should review and update its curriculum immediately, adding practical lessons on data laws and internet safety so that graduates are fully prepared to handle digital office files securely before they get a job.

Contribution to Knowledge

The study has contributed to knowledge by providing fresh empirical evidence on the behavioural gaps in data security within higher education administration, rather than focusing purely on IT infrastructures. By comparing federal and state tertiary institutions under the Nigeria Data Protection Act (NDPA), it identified specific operational differences in how administrative personnel manage sensitive institutional registries. Most importantly, the study has bridged the gap between

organisational behaviour and curriculum development, offering a data-backed blueprint that shows exactly why they Business Education curriculum should be updated to train a resilient, security-conscious workforce capable of handling modern digital threats.

Implications for Business Education

The findings carry profound implications for business education framework within the public sector. For decades, office Management training focused heavily on speed, accuracy, and basic clerical workflows. However, the disparities found between federal and state indicate that modern office professionals can no longer just be efficient typists; they should be competent data custodians. When office staff lack strong security habits, the entire digital infrastructure of a university becomes vulnerable to leaks, regardless of how expensive the institution's firewall software is. To protect sensitive institutional databases, Business Education practices should shift from passive data entry to active, security-conscious information management. Furthermore, these findings indicate that a major shift is required in how office technologies are taught and managed in the classroom. If office technology management training programmes fail to teach practical risk management alongside software applications, they will continue to produce graduates who view security protocols as a slow chore rather than a vital professional duty. For the Department of Business Education, this means that data governance, password safety, email verification, and compliance with the NDPA should become permanent elements of secretarial trainings. Most importantly, if Business Education modules are not updated to reflect these modern digital threats, public institutions will continue to face an uneven security and scape, leaving state-level offices exposed to severe operational and legal penalties.

REFERENCES

Abawajy, J. H. (2014). User preference of cybersecurity awareness delivery methods. *Behaviour & Information Technology, 33*(3), 237-248.

Albrechsten, E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26*(4), 276-289.

Altbach, P. G. (2005). The private higher education revolution: An introduction. In P. G. Altbach & D. C. Levy (Eds.). *Private higher education: A global revolution* (pp. 1-12). Sense publishers.

Altman, I. (1975). *The environment and social behaviour: Privacy, personal space, territory, crowding*. Brooks/Cole Publishing Company.

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2025). Cybersecurity awareness campaigns: Why they fail to change behaviour. *International conference on cybersecurity for sustainable society* (pp.118-131).

Bassey, A. S., & Ebieme, E. E. (2026). Integration of artificial intelligence into the Business education programmes: A Panacea for building a technological driven workforce. *Studies in Education, 24*(1), 95-102.

Blau, P. M., & Scott, W. R. (1962). *Formal organizations: A comparative approach*. Chandler Publishing Company.

Brooks, D. C., & McCormack, M. (2020). *Driving digital transformation in higher education*. EDU CAUSE Research.

Bulgurcu, B., Cavvsoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.

Charles, C. I., & Etuk, O. U. (2016). Business education and acquisition of marketable skills: implications for self-reliance by Nigerian Youths. *Journal of Education, 9*(1), 247-256.

Chikwendu, S. C., & Oli, N. P. (2023). Human factors influencing compliance to cybersecurity practices by employees of public universities in southeast Nigeria. *International Journal of Information Security, Privacy and Digital Forensics, 7*(1), 44-58.

Clarke, A., & Chalmers, D. (1998). *The extended mind. Analysis, 58*(1), 7-19.

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative and mixed methods approaches* (5th ed.). Sage Publications.

Cronbach, I. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika, 16*(3), 297.334.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59*(3), 323-342.

D'Arcy, J., Hovav, A., & Galleta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79-98.

Dabai, D. S., & Ibrahim, A. (2026). Comparative study on awareness and application of cybersecurity practices between federal and state tertiary institutions in Kebbi State, Nigeria: *International Journal of Progressive Research in Engineering Management and Science, 6*(9), 1-12.

Drucker, P. F. (1999). *Management challenges for the 21st century*. Harper Business.

Ebieme, E. E. (2026). Strategic human resource management and organisational performance in the Nigerian National Assembly: Implications for Business Education Curriculum. *Uniuyo Journal of Business Education and Entrepreneurship, 3*(2), 62-71.

Ebieme, E. E., & Bassey, A. S. (2026). Evaluating the role of emotional intelligence in employees' job performance in First Bank, Akwa Ibom North-East, Nigeria. *African Journal of Management and Business Research, 22*(1), 367-383.

Ebieme, E. E., & Daniel, S. F. (2026). Digital communication competencies and undergraduate Business Education students' employment readiness at the University of Uyo, Akwa Ibom State, Nigeria. *Kogi Journal of Education and Pedagogy, 5*(1), 181-190.

Ebieme, E. E., & Enyetip, I. A. (2026). Administrative artificial intelligence and secretarial staff job performance in Nigerian commercial banks:

Implications for Business Education curriculum. *Unizik Journal of Educational Research, Science and Vocational Studies, 5*(1), 386-398.

Ebieme, E. E., & Umana, S. A. (2026). Strategic intelligence and organisational crisis management: Evidence from Pension Fund Administrators in Akwa Ibom State, Nigeria. *African Journal of Management and Business Research, 23*(1), 283-300.

Ebieme, E. E., Imagha, O. A., Robert, O. G., & Atakpo, E. U. (2024). Self-awareness and Business Educators' job performance in Federal Universities in South-South, Nigeria. *International Journal of Business and Management Review, 12*(3), 18-38.

Ebieme, E. E., Udokang, I. A., & Offong, T. C. (2026). Compensation packages and Access Bank employees' job performance in Akwa Ibom State, Nigeria. *AAU Journal of Business Educators, 6*(1), 1-8.

Ebieme, E. E., Umana, S. A., & Chidi, C. P. (2026). Integrating human resource analytics into Business Education curriculum: Perspectives of senior human resource managers in Akwa Ibom State, Nigeria. *East African Journal of Education Studies, 9*(4), 113-128.

Edoho, O. G., Akpotu, N. E., & Asiyai, R. I. (2025). Registry best practices and administrative effectiveness: Empirical evidence and comparative insights from Nigerian Universities. *International Journal of Educational Management and Development Studies, 6*(2), 45-61.

Enyetip, I. A., & Ebieme, E. E. (2026). Human resource management practices and teachers' job performance in public secondary schools in Uyo Local Government Area, Akwa Ibom State, Nigeria. *African Journal of Educational Management, Teaching and Entrepreneurship Studies, 16*(1), 327-347.

Enyetip, I. A., & Ebieme, E. E. (2026). Employee relations and organisational effectiveness: Evidence from Akwa Ibom State Civil Service, Nigeria. *International Journal of Management Science and Business Analysis Research, 12* (7), 145-163.

Federal Republic of Nigeria (2023). *Nigeria Data Protection Act, 2023 (Acts No. 24,* Government Notice No. 37, Gazette No. 110). Federal Government Printer, ndpc.gov.ng.

Furnell, S. M., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal internet users. *Computer & Security, 26*(5), 410-417.

Gornitzka, A., & Larsen, I. M. (2004). Towards professionalisation? Restructuring of administrative workforce in Universities. *Higher Education, 47*(4), 455-471.

Greenaway, K. E., Chan, Y. E., & Crossler, R. E. (2015). Company information privacy orientation: A conceptual framework. *Information systems Journal, 25*(6), 579-606.

Hadlington, L. (2018). Employee's attitudes towards cybersecurity and risky online behaviours: An empirical assessment in the United Kingdom. *International Journal of Cyber Criminology, 11*(2), 266-281.

Heinrich, M. W., & Gerhart, N. (2023). Privacy education effectiveness: Does it matter? *Journal of Information Systems Education, 34*(1), 49-69.

Imagha, O. A., & Ebieme, E. E. (2024). Evaluating the influence of self-regulation on job performance in Champion Brewery, Plc, Uyo, Akwa Ibom State, Nigeria. *International Journal of Research and Scientific Innovations, 10*(6), 136-141.

Irish, A. L., Gazica, M. W., & Decerra, V. (2025). A qualitative descriptive analysis on generative artificial intelligence: Bridging the gap in pedagogy to prepare students for the workplace. *Discover Education, 4*(1), 1-15.

Katz, D., & Kahn, R. L. (1978). *The social psychology of organizations (2nd ed.).* Wiley.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289-296.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly, 33*(1), 71-90.

Liginlal, D., Sim, I., & Khansa, L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers & Security; 28*(3), 215-228.

Marguis, C. (2003). The pressure of the past: Network imprinting intercorporate communities. *Administrative Science Quarterly, 48*(4), 655-689.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., Slapnis, M. (2017). Individual differences and information security awareness. *Computers & Security, 69*,151-156.

Mintzberg, H. (1979). *The structuring of organisations: A synthesis of the research*. Prentice-Hall.

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory (3rd ed.).* McGraw-Hill.

Nworgu, B. G. (2015). *Educational research: Basic issues and methodology (3rd ed.).* University Trust Publisher.

Oyefeso, O. O., & Saleh, A. (2025). The role of cybersecurity in safeguarding digital systems in institution of higher learning. *Kontagora Journal of Intellectual Discourse, 3*(1), 280-292.

Parsons, K., McCormax, A., Pattinson, M., Butavicius, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42,* 165-176.

Rhoades, G. (1998). *Managed professionals: Unionized faculty and restructuring academic labor.* State University of New York Press.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93-114.

Salam, M., Abubakar, K. A., Abdul Ghani, A. T., & Mohd Aman, A. H. (2026). Cybersecurity in higher education institutions digitalisation: Addressing threats and vulnerabilities. *SAGE Open, 16*(1), 1-14.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J.

(2009). The impact of information richness on information security awareness training effectiveness. *Information & Management, 46*(2), 92-97.

Simon, H. A. (1997). *Administrative behaviour (4th ed.)*. Free Press.

Siponen, M. T. (2000). A conceptual foundation for organisational information security awareness. *Information Management & Computer Security, 8*(1), 31-41.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individual's concerns about organisational practices. *MIS Quarterly, 20*(2), 167-196.

Solove, D. J. (2006). A taxanomy of privacy. *University of Pennsylvania Law Review, 15*(4), 477-564.

Spiekerman, S., & Cranor, L. F. (2009). Engineering privacy. *IEEE Transactions on Software Engineering, 35*(1), 67-82.

Szekeres, J. (2011). Professional staff carve out a new space. *Journal of Higher Education Policy and Management, 33*(6), 679-691.

Ugo-Onyeka, O. D., Maduka, O. I., Mogbeyiteren, O. L. B., & Ojedokun, F. S. A. (2026). Cybersecurity readiness and data protection practices in Nigerian tertiary institutions. *Spanish Journal of Innovation and Integrity, 53,* 7-15.

Ukoima, E. F., Etuk, O. U., & Charles, C. I. (2025). Business programmes in Nigeria: Challenges, way forward and strategies for curbing economic uncertainties. *Journal of Association of Vocational and Technical Educators of Nigeria, 2*(1) 219-229.

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems, 28*(2), 118-144.

Westin, A. F. (1967). *Privacy and Freedom.* Atheneum.

Whitchurch, C. (2008). Shifting identities and blurring boundaries: The emergence of third space professionals in UK higher education: *Higher Education Quarterly, 62*(4), 377-396.