International Journal of Management Technology, 13(2), 73-90, 2026
Print ISSN: ISSN 2055-0847(Print)
Online ISSN: ISSN 2055-0855(Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Information Security Culture and Cybersecurity Policy Compliance in The University of Abuja: The Mediating Role of Cybersecurity Awareness

Akinsola Racheal Oluwabunmi, Sonia Sim Joshua, Atinuke Funmilayo Opeseitan, Osaro Cynthia Ojo
Department of Business Administration, Nile University of Nigeria Abuja

doi: https://doi.org/10.37745/ijmt.2013/vol13n27390 Published July 16, 2026

Citation: Oluwabunmi A.R., Joshua S.S., Opeseitan A.F., Ojo O.C. (2026) Information Security Culture and Cybersecurity Policy Compliance in The University of Abuja: The Mediating Role of Cybersecurity Awareness, *International Journal of Management Technology*, 13(2), 73-90

Abstract: *The escalating prevalence of human-mediated cybersecurity incidents in higher education institutions underscores the inadequacy of purely technological defences and redirects scholarly and policy attention toward behavioural and cultural antecedents of compliance. This paper examines the effect of Information Security Culture (ISC), operationalised through Cyber Security Education, Training and Awareness (CSETA), on Cybersecurity Policy Compliance (CPC) among staff and students of the University of Abuja, Nigeria, with Cybersecurity Awareness as a mediating variable. The University of Abuja provides a particularly instructive institutional setting, as a federal dual-mode university whose residential and distance learning operations expose a heterogeneous user community of approximately 58,726 staff and students to intensifying cyber threats within an evolving Nigerian regulatory environment. The problem of persistent policy non-compliance, despite the enactment of the Nigeria Data Protection Act (2023) and related national cybersecurity instruments, constitutes the motivating research problem. The study aims to examine how CSETA influences three sub-dimensions of compliance, namely Incident Response Behaviour (IRB), Data Handling and Protection (DHP), and Intention to Comply with Security Policies (ITC), and to evaluate whether these relationships operate through the cognitive mediation of cybersecurity awareness. Three established behavioural paradigms provide the theoretical foundation: Protection Motivation Theory (Rogers, 1975, 1983), General Deterrence Theory (Gibbs, 1975; Straub, 1990), and the Theory of Planned Behaviour (Ajzen, 1991). A cross-sectional quantitative design will be employed, with a stratified random sample of 400 respondents drawn proportionally from the staff and student populations. Data will be collected through a validated 33-item structured questionnaire. Multiple regression analysis will test the direct effects at $p < .05$, while the Hayes (2022) PROCESS Macro Model 4 with 5,000 bias-corrected bootstrap resamples will test the mediating role of cybersecurity awareness. The study is expected to contribute a theoretically integrated, empirically grounded, and contextually relevant evidence base for cybersecurity governance within Nigerian federal universities, address significant gaps in the higher education cybersecurity compliance literature, and offer actionable guidance for institutional policy and practice.*

Keywords: information security culture, cybersecurity policy compliance, cybersecurity awareness, CSETA, higher education, Nigeria, mediation analysis

International Journal of Management Technology, 13(2), 73-90, 2026
Print ISSN: ISSN 2055-0847(Print)
Online ISSN: ISSN 2055-0855(Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

INTRODUCTION

The progressive digitalisation of higher education has transformed universities into repositories of high-value information assets, while simultaneously extending their exposure to an increasingly sophisticated cyber threat landscape. Global industry evidence underscores the urgency of this challenge: the average cost of a single data breach now stands at approximately USD 4.88 million, and the human element is implicated in approximately 68 percent of recorded breaches, a proportion that has remained remarkably stable across successive reporting cycles (IBM Security, 2024; Verizon, 2024). These statistics compel a recalibration of institutional cybersecurity strategy from a predominantly technical orientation toward an understanding of the behavioural and cultural mechanisms that determine whether formal security controls translate into routine compliant behaviour.

In Nigeria, this challenge is intensified by the rapid expansion of the digital economy, with active internet subscriptions estimated at over 160 million as of 2024 (Nigerian Communications Commission [NCC], 2024), and by the country's elevated exposure to cybercrime, including phishing, business email compromise, and ransomware (Cyber Security Experts Association of Nigeria [CSEAN], 2023). The legislative architecture governing cybersecurity in Nigerian institutions has matured significantly, encompassing the Cybercrimes (Prohibition, Prevention, etc.) Act (2015, as amended in 2024), the Nigeria Data Protection Act (2023), and the National Cybersecurity Policy and Strategy (2021). Yet a persistent gulf exists between formal regulatory prescription and the behavioural conduct of users within Nigerian public institutions, particularly universities. The INTERPOL African Cyberthreat Assessment (2024) identifies online scams, business email compromise, and ransomware as the dominant threat categories across the continent, and attributes the comparatively low incident reporting rates in African higher education institutions, in part, to deficiencies in user awareness and security culture.

The University of Abuja constitutes a particularly instructive empirical setting within this context. Established in 1988 and formally operating as a federal dual-mode institution offering both conventional and distance learning programmes, the university serves approximately 58,726 staff and students across its Main Campus on the Abuja-Airport Road and its Mini Campus in Gwagwalada Area Council (University of Abuja, n.d.). The institution was rebranded as Yakubu Gowon University in 2024, though the founding name remains in widespread administrative usage. The dual-mode character of the university, which circulates substantial volumes of administrative and academic data through digital channels spanning multiple geographies and end-user profiles, materially amplifies its ICT exposure. Within this setting, the question of how to cultivate behavioural compliance with cybersecurity policies among a heterogeneous and geographically distributed user community has emerged as both an institutional imperative and a research priority. The study is anchored upon three interrelated constructs. The independent variable, Information Security Culture (ISC), is operationalised through Cyber Security Education, Training and

Awareness (CSETA), the structured organisational mechanism most directly responsible for shaping the values, knowledge, and behavioural expectations associated with secure ICT use (Hassandoust et al., 2022). The dependent variable, Cybersecurity Policy Compliance (CPC), is conceptualised across three sub-dimensions: Incident Response Behaviour (IRB), Data Handling and Protection (DHP), and Intention to Comply with Security Policies (ITC) (Alraja et al., 2023; Aigbefo et al., 2022). The mediating variable, Cybersecurity Awareness, is operationalised through Knowledge of Cybersecurity Policies and Procedures, capturing the cognitive bridge through which cultural inputs translate into compliant behavioural outputs (Tran et al., 2024; Hong & Furnell, 2022).

Several research gaps motivate the present investigation. First, the empirical literature on cybersecurity policy compliance is dominated by studies conducted in corporate, banking, healthcare, and governmental settings, with a relative under-representation of higher education institutions and an even sparser evidence base drawn from Nigerian or West African universities (Yusif & Hafeez-Baig, 2023; Tran et al., 2025). Second, the mediating role of cybersecurity awareness in the relationship between security culture and policy compliance, while theoretically well-supported, has rarely been subjected to formal mediation testing within Nigerian university contexts using contemporary bootstrap-based procedures (Hayes, 2022). Third, most existing studies sample academic and administrative staff while excluding students, despite students constituting the dominant ICT user group in most universities (Ahamed et al., 2024; Yusif & Hafeez-Baig, 2023). The present study addresses these gaps by drawing upon a stratified sample of staff and students from the University of Abuja and testing a theoretically integrated mediated model through the Hayes PROCESS Macro Model 4.

The study is guided by four research questions: (i) To what extent does CSETA affect Incident Response Behaviour among staff and students of the University of Abuja? (ii) To what extent does CSETA affect Data Handling and Protection? (iii) To what extent does CSETA affect Intention to Comply with Security Policies? (iv) To what extent does Cybersecurity Awareness mediate the relationship between CSETA and Cybersecurity Policy Compliance? These questions are pursued through four corresponding null hypotheses tested at the five percent level of significance. The paper is organised as follows: Section 2 presents the literature review; Section 3 develops the conceptual framework and hypotheses; Section 4 describes the methodology; Section 5 discusses expected contributions; and Section 6 provides a conclusion.

LITERATURE REVIEW

Conceptual Review

Information Security Culture and CSETA

Information Security Culture (ISC) is conceptualised as a domain-specific manifestation of organisational culture, encompassing the shared assumptions, values, attitudes, and behavioural

norms that influence how members of an organisation perceive and act upon security-related obligations (Hassandoust et al., 2022; Yusif & Hafeez-Baig, 2023). Drawing upon the tripartite model of organisational culture, ISC operates across three interlocking layers: visible artefacts (observable security practices and policy documents), espoused values (stated principles governing security decisions), and underlying basic assumptions (largely tacit beliefs about the legitimacy and feasibility of information security obligations). The practical significance of ISC lies in its role as the social and cognitive substrate upon which formal security controls operate; it determines whether written policies translate into routine behaviour or remain inert artefacts of institutional governance (Hassandoust et al., 2022).

The most directly observable and policy-actionable dimension of ISC in the higher education context is Cyber Security Education, Training and Awareness (CSETA). The NIST (2003) canonical model distinguishes three interlinked activities within CSETA: awareness (ensuring cognitive salience of security obligations), training (developing specific security competencies), and education (integrating skills and knowledge into broader professional judgement). Contemporary empirical work confirms that well-designed CSETA programmes significantly improve compliance with information security policies, with design features such as task relevance, modality variety, repetition, and integration with accountability systems emerging as particularly consequential for behavioural impact (Mou et al., 2022; Tran et al., 2024). Within higher education specifically, the heterogeneous user community encompassing academic staff, administrative personnel, and students necessitates differentiated CSETA strategies rather than monolithic awareness messaging (Ahamed et al., 2024; Yusif & Hafeez-Baig, 2023).

Cybersecurity Policy Compliance

Cybersecurity Policy Compliance (CPC) refers to the extent to which members of an organisation behaviourally and intentionally adhere to the cybersecurity policies, procedures, and standards prescribed by their institution (Alraja et al., 2023; Arif et al., 2025). The construct combines an action-oriented behavioural component, observable in routine ICT use, with an attitudinal-intentional component captured through respondents' stated dispositions toward policy adherence. The present study operationalises CPC across three sub-dimensions that represent the most consequential compliance domains in higher education settings.

Incident Response Behaviour (IRB) denotes the actions an individual undertakes when confronted with a perceived or actual cybersecurity incident, including timely reporting to appropriate institutional channels, escalation through prescribed procedures, and containment actions (Aigbefo et al., 2022; Alraja et al., 2023). Data Handling and Protection (DHP) captures the behavioural practices by which an individual secures data in conformity with institutional cybersecurity and data protection policies, integrating three foci: prevention of unauthorised access, prevention of unauthorised disclosure, and prevention of unauthorised modification or destruction (Tran et al., 2024; Federal Republic of Nigeria, 2023). Intention to Comply with Security Policies (ITC) captures an individual's stated behavioural disposition to adhere to prescribed cybersecurity

policies (Ajzen, 1991; Hong & Furnell, 2022), which within the Theory of Planned Behaviour functions as the proximal antecedent of actual compliance behaviour.

Cybersecurity Awareness

Cybersecurity Awareness refers to the conscious cognitive state in which members of an organisation possess accurate knowledge of cybersecurity risks, policies, and procedures, and recognise the relevance of this knowledge to their everyday ICT practices (Tran et al., 2025; Ahamed et al., 2024). Two principal conceptualisations have shaped the literature. The first treats awareness as general security mindfulness, capturing the extent to which an individual recognises the personal relevance of information security obligations an approach associated with Bulgurcu et al. (2010), whose highly cited study demonstrated that information security awareness significantly shapes the attitudes and beliefs governing compliance intention. The second conceptualises awareness as domain-specific knowledge, operationalised by Parsons et al. (2014) through the Human Aspects of Information Security Questionnaire (HAIS-Q). The present study adopts the latter approach, operationalising cybersecurity awareness through Knowledge of Cybersecurity Policies and Procedures, which captures the cognitive bridge through which cultural and educational inputs translate into compliant behavioural outputs.

Theoretical Review

Three established behavioural paradigms anchor the theoretical foundation of the present study, each contributing a distinctive explanatory pathway to the phenomenon of cybersecurity policy compliance.

Protection Motivation Theory

Protection Motivation Theory (PMT), advanced by Rogers (1975) and revised by Rogers (1983), explains how individuals form intentions to engage in protective behaviour through two cognitive appraisal processes. Threat appraisal evaluates the maladaptive response, comprising perceived severity and perceived vulnerability, partially offset by the rewards associated with non-compliance. Coping appraisal evaluates the adaptive response, comprising response efficacy, self-efficacy, and response costs. Higher perceived severity, vulnerability, response efficacy, and self-efficacy, alongside lower response costs, jointly produce stronger protective intentions and behaviour. PMT has been extensively validated within cybersecurity behavioural research (Mou et al., 2022), with meta-analytic evidence confirming that coping appraisal variables, particularly self-efficacy and response efficacy, are among the most consistent predictors of security-related intentions. CSETA directly cultivates both threat appraisal (by communicating the nature and likelihood of cyber threats) and coping appraisal (by equipping users with the knowledge and skills to respond protectively), making PMT a critical explanatory lens for the CSETA-compliance relationship.

General Deterrence Theory

General Deterrence Theory (GDT), systematised by Gibbs (1975) and introduced into the information systems domain by Straub (1990), posits that the likelihood of rule-violating

behaviour is reduced when the perceived costs — expressed as the certainty, severity, and celerity of formal sanctions — outweigh the perceived benefits. Straub (1990) demonstrated that organisations employing visible deterrence mechanisms experienced significantly lower rates of computer misuse. Contemporary meta-analytic evidence confirms that sanction certainty exerts a more consistent deterrent influence than severity (Hengstler et al., 2023). CSETA intersects with GDT by cultivating awareness of the institutional and legal sanctions associated with policy non-compliance, thereby raising the perceived costs of non-compliant behaviour and suppressing the likelihood of policy violation.

Theory of Planned Behaviour

The Theory of Planned Behaviour (TPB), formulated by Ajzen (1991), posits that behavioural intention — the proximal antecedent of behaviour — is determined by three cognitions: attitudes (the individual's overall evaluation of the behaviour), subjective norms (perceived social pressure to comply), and perceived behavioural control (the individual's perceived ease or difficulty in performing the behaviour). TPB has been extensively validated as a predictor of security policy compliance intention across diverse organisational contexts (Aigbefo et al., 2022; Hong & Furnell, 2022), and integrated models combining TPB with PMT and GDT have demonstrated superior explanatory power over single-theory specifications (Alam et al., 2024). CSETA programmes directly cultivate the TPB cognitions by shaping favourable attitudes toward compliance, reinforcing subjective norms through institutional communication, and enhancing perceived behavioural control through skills development.

The three theories are theoretically complementary and mutually reinforcing. PMT contributes the motivational pathway through threat and coping appraisals; GDT contributes the sanction-perception pathway; and TPB contributes the attitudinal-normative pathway. Their integration within a single mediated model provides a richer theoretical foundation than any single framework considered in isolation, and aligns with the growing scholarly consensus that cybersecurity compliance research benefits from theoretical synthesis rather than the isolated testing of competing paradigms (Mou et al., 2022; Alam et al., 2024).

Empirical Review

CSETA and Incident Response Behaviour

A substantial body of evidence supports the positive relationship between CSETA and incident response behaviour. Contemporary empirical work demonstrates that user awareness of security education, training, and awareness programmes significantly increases perceived sanctions for misuse and reduces reported computer misuse intentions (Arif et al., 2025; Alraja et al., 2023). Within higher education contexts, cybersecurity awareness and information security policy compliance have been found to significantly enhance user reporting of suspicious messages and adherence to incident response protocols, with programme quality and frequency functioning as significant moderators (Oroni et al., 2025; Ahamed et al., 2024). Nigerian and broader African evidence, while primarily drawn from policy and industry reports rather than peer-reviewed empirical investigations, is consistent with the international literature: the CSEAN (2023) reports

that institutions maintaining regular awareness programmes experience higher incident reporting rates and more rapid containment of security events, while INTERPOL (2024) attributes the persistently low incident reporting rates in African higher education to gaps in user awareness.

CSETA and Data Handling and Protection

The relationship between CSETA and data handling and protection is among the most extensively researched dependencies in behavioural cybersecurity research. Contemporary empirical work demonstrates that information security awareness significantly enhances the rationality-based beliefs governing data handling compliance, and that compliance intention significantly predicts self-reported data-handling behaviour (Alraja et al., 2023; Aigbefo et al., 2022). Meta-analytic evidence identifies information security awareness as among the most consistently significant predictors of data-protection compliance, with robust effect sizes across sectors, organisational sizes, and measurement approaches (Hengstler et al., 2023). Higher-education-specific evidence confirms that CSETA-mediated awareness significantly predicts data-handling compliance, with inadequate awareness identified as a pervasive institutional vulnerability (Yusif & Hafeez-Baig, 2023; Oroni et al., 2025). The promulgation of the Nigeria Data Protection Act (2023) has elevated the policy salience of this relationship, establishing direct legal obligations for data controllers and processors, including educational institutions.

CSETA and Intention to Comply with Security Policies

Compliance intention is the most extensively studied outcome in the behavioural cybersecurity literature, and the CSETA-intention relationship is correspondingly well-established. Contemporary empirical work reports that information security awareness is a significant antecedent of compliance intention, operating through its effects on attitudes, normative beliefs, and self-efficacy (Hong & Furnell, 2022). Integrated multi-theory studies demonstrate that CSETA exposure significantly enhances compliance intention, with depth and frequency of exposure functioning as significant predictors across multiple organisational contexts (Alam et al., 2024). Unified-model studies further confirm that awareness remains a significant antecedent of compliance intention after controlling for PMT, GDT, normative, and self-regulation variables (Alrawhani et al., 2025). Within higher education, the cultivation of compliance intention among a heterogeneous user population requires differentiated awareness approaches sensitive to the distinct roles, prior knowledge, and ICT exposure of staff and students (Ahamed et al., 2024).

Mediating Role of Cybersecurity Awareness

The proposition that cybersecurity awareness mediates the relationship between cultural and educational inputs and compliance outcomes is theoretically over-determined: each of the three behavioural paradigms reviewed above converges upon this role. Within PMT, awareness contributes to the threat and coping appraisal cognitions that govern protection motivation (Han et al., 2025). Within GDT, awareness of policies and procedures is a necessary cognitive precondition for the perception of sanctions to influence behaviour (Hengstler et al., 2023; Arif et al., 2025). Within TPB, awareness shapes the attitudes, subjective norms, and perceived behavioural control that produce compliance intention (Ajzen, 1991; Hassandoust et al., 2022). Empirically,

contemporary PLS-SEM evidence demonstrates that cybersecurity awareness partially mediates the relationship between organisational variables and information security behaviour, accounting for a substantive share of the total effect (Oroni et al., 2025; Tran et al., 2025). The literature identifies Bulgurcu et al. (2010) and subsequent studies as establishing awareness as a recurring intervening variable, while noting that formal mediation tests using bootstrap-based procedures remain comparatively rare, particularly within Nigerian higher education contexts.

Knowledge Gap

The synthesis of the conceptual, theoretical, and empirical evidence reveals six interrelated gaps that the present study seeks to address. Conceptually, there is a lack of consensus on the measurement of ISC in higher education settings, with existing operationalisations rarely validated within Nigerian federal universities. Theoretically, the joint integration of PMT, GDT, and TPB within a single mediated model has not been applied to cybersecurity compliance within a Nigerian federal dual-mode university. Empirically, the literature is dominated by studies set in corporate and governmental contexts in North America, Europe, and East Asia, with Nigerian universities and the University of Abuja in particular virtually absent from the peer-reviewed evidence base. Methodologically, the application of the Hayes (2022) PROCESS Macro Model 4 with bias-corrected bootstrap confidence intervals to mediation testing in this context has not been reported. At the population level, students who constitute the dominant ICT user group in most universities have been systematically under-represented in cybersecurity compliance research. Finally, at the practitioner level, there exists a significant knowledge void regarding the relative contributions of cultural and cognitive antecedents to compliance, leaving institutional managers without evidence-based guidance for cybersecurity investment decisions.

CONCEPTUAL FRAMEWORK AND HYPOTHESES DEVELOPMENT

Drawing upon the conceptual and theoretical review, the present study proposes a mediated model in which CSETA — as the operational expression of Information Security Culture — exerts both direct and indirect effects on Cybersecurity Policy Compliance, with Cybersecurity Awareness operating as the cognitive mediator. The conceptual framework, anchored in Bulgurcu et al. (2010), Cram et al. (2019), Da Veiga et al. (2020), and Hayes (2022), specifies three direct paths and one indirect path.

The direct paths correspond to the first three hypotheses: CSETA is expected to exert a positive and significant influence on Incident Response Behaviour (path 1), on Data Handling and Protection (path 2), and on Intention to Comply with Security Policies (path 3). These direct effects are explained by all three theoretical paradigms. Under PMT, CSETA cultivates the threat appraisal and coping appraisal cognitions that motivate protective behaviour. Under GDT, CSETA raises awareness of the sanctions associated with non-compliance, suppressing the perceived attractiveness of policy violation. Under TPB, CSETA shapes the attitudes, subjective norms, and perceived behavioural control that translate into compliance intention.

The indirect path corresponds to the fourth hypothesis and models the mediating mechanism through which CSETA influences the composite CPC score. CSETA first influences Cybersecurity Awareness (path a), by enhancing respondents' knowledge of cybersecurity policies and procedures. Cybersecurity Awareness then influences Cybersecurity Policy Compliance (path b), by translating cognitive accessibility of security knowledge into compliant behavioural outputs. The indirect effect, estimated as the product of paths a and b, captures the portion of CSETA's total effect on compliance that operates through the cognitive intermediary of awareness.

The mediated structure of the model is consistent with the neo-institutional, motivational, and attitudinal-normative pathways identified in the theoretical review. The model anticipates partial rather than full mediation, given the theoretical expectation that CSETA also exerts a direct influence on compliance through deterrence and attitudinal mechanisms that do not require the cognitive mediation of awareness. The framework integrates the institutional and behavioural levels of analysis, positioning CSETA as the organisational lever through which ISC is transmitted, awareness as the cognitive mechanism through which that transmission operates, and the three compliance sub-dimensions as the behavioural and intentional outcomes that the model seeks to explain.

The following four null hypotheses are formulated and will be tested at the five percent level of significance:

H_{01}: CSETA has no significant effect on Incident Response Behaviour among staff and students of the University of Abuja.

H_{02}: CSETA has no significant effect on Data Handling and Protection among staff and students of the University of Abuja.

H_{03}: CSETA has no significant effect on Intention to Comply with Security Policies among staff and students of the University of Abuja.

H_{04}: Cybersecurity Awareness has no significant mediating effect on the relationship between CSETA and Cybersecurity Policy Compliance among staff and students of the University of Abuja.

METHODOLOGY

The study adopts a cross-sectional quantitative research design embedded within a positivist research philosophy. Positivism holds that social and behavioural phenomena are amenable to objective measurement and that causal relationships among variables can be inferred from empirical data through rigorous statistical procedures Clark et al. (2022). This philosophical orientation supports the use of validated multi-item instruments, deductive hypothesis testing, and inferential statistical analysis. The cross-sectional design, which captures data at a single point in time across a heterogeneous sample, is appropriate for examining the strength and direction of

relationships among constructs and for testing theoretically derived hypotheses about the determinants of compliance behaviour (Creswell & Creswell (2023).

The study population comprises all staff and students of the University of Abuja who interact with the institution's ICT systems and are subject to its cybersecurity policies during the 2024/2025 academic session. This constitutes a total population of 58,726, comprising 3,362 academic and non-academic staff and 55,364 students enrolled across conventional and distance learning programmes. The sample size is determined using the Krejcie and Morgan (1970) formula, which yields a minimum required sample of approximately 382 for a population of this size at the five percent margin of error and 95 percent confidence level. To accommodate anticipated non-response, enhance statistical power, and ensure adequate within-stratum sample sizes, the calculated minimum is rounded upward to 400. This sample size satisfies the conventional ratio of 10 to 20 cases per parameter recommended for multiple regression analysis Hair et al. (2022) and exceeds the minimum sample of 200 recommended for bootstrap-based mediation analysis (Hayes, 2022). Stratified random sampling with proportional allocation is employed, with the principal stratification variable being institutional role (staff versus students). Proportional allocation distributes the sample of 400 across strata in proportion to each stratum's share of the total population, yielding 23 staff respondents and 377 student respondents. Within each principal stratum, further sub-allocation proceeds proportionally across campus and faculty or organisational unit. Random selection within each sub-stratum is implemented through systematic random sampling from the institutional staff list and student register, accessed under formal institutional permission.

Primary data are collected through a structured self-administered questionnaire comprising 33 items across six sections. Section A captures demographic and ICT-experience information. Sections B through F operationalise the five principal constructs of the study: CSETA (6 items), Cybersecurity Awareness (5 items), Incident Response Behaviour (5 items), Data Handling and Protection (5 items), and Intention to Comply with Security Policies (5 items). All construct items are measured on a five-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree). Items in Sections B to F are adapted from validated scales in the established cybersecurity behavioural literature (NIST, 2003; Aigbefo et al., 2022; Alraja et al., 2023; Hong & Furnell, 2022; Tran et al., 2024, 2025), with adaptations limited to terminology and contextual reference to preserve conceptual fidelity while reflecting the higher education setting of the University of Abuja. The questionnaire is administered in both physical (paper-based) and electronic (web-based) formats to accommodate the dual-mode operational character of the institution.

Content validity is established through a structured expert review by a panel of five specialists, comprising two academics in information systems or cybersecurity, two practising information security professionals, and one research methodologist. Each expert rates the relevance of each item on a four-point scale. The Content Validity Index for each item (I-CVI) is required to meet or exceed 0.78, and the Scale Content Validity Index averaged across items (S-CVI/Ave) is required to meet or exceed 0.90 Kang et al. (2023). Construct validity is established through

confirmatory factor analysis, with convergent validity assessed through standardised factor loadings (≥ 0.70) and Average Variance Extracted (AVE ≥ 0.50; Fornell & Larcker, 1981), and discriminant validity assessed through the Fornell-Larcker criterion and the Heterotrait-Monotrait (HTMT) ratio (< 0.85; Henseler et al., 2015). Model fit is evaluated using the Comparative Fit Index (CFI ≥ 0.90), Tucker-Lewis Index (TLI ≥ 0.90), Root Mean Square Error of Approximation (RMSEA ≤ 0.08), and Standardised Root Mean Square Residual (SRMR ≤ 0.08; Hu & Bentler, 1999). Reliability is established through Cronbach's alpha (threshold ≥ 0.70; Nunnally, 1978) and Composite Reliability (threshold ≥ 0.70; Hair et al., 2022). Procedural and statistical remedies for common-method bias include respondent anonymity, item-order controls, and Harman's single-factor test. A two-stage instrument refinement process comprising pretesting (5–10 respondents from a comparable institution) and a pilot study (30–50 respondents from a distinct Nigerian federal university) is conducted prior to the main data collection phase to establish initial reliability and construct validity statistics and to refine item wording, ordering, and presentation.

All analyses are conducted using IBM SPSS Statistics version 26, with the Hayes (2022) PROCESS Macro version 4 installed as an extension. Data preparation encompasses screening for completeness, missing data treatment through mean substitution or expectation-maximisation imputation (depending on the pattern assessed through Little's MCAR test), reverse-coding where applicable, and computation of unweighted construct scale scores. Descriptive statistics — frequencies, percentages, means, standard deviations, skewness, and kurtosis — summarise the sample profile and construct distributions. Diagnostic analyses evaluate the standard regression assumptions of normality, homoscedasticity, independence, linearity, and absence of multicollinearity, using Variance Inflation Factor (VIF < 5), tolerance (> 0.20), Durbin-Watson statistics, and Cook's distance.

The first three null hypotheses are tested through multiple regression analysis, with each compliance sub-dimension (IRB, DHP, and ITC) regressed on CSETA with demographic variables as controls. The null hypothesis is rejected at $p < .05$ (two-tailed). Effect sizes are interpreted according to Cohen's (1988) conventions. The fourth null hypothesis is tested through the Hayes (2022) PROCESS Macro Model 4, which simultaneously estimates path a (the effect of CSETA on Cybersecurity Awareness), path b (the effect of Cybersecurity Awareness on composite CPC controlling for CSETA), and the direct effect c' (the effect of CSETA on CPC controlling for Cybersecurity Awareness). The indirect effect ($a \times b$) is estimated using 5,000 bootstrap resamples with bias-corrected and accelerated 95 percent confidence intervals. The null hypothesis of no mediation is rejected if the confidence interval does not contain zero. Supplementary analyses evaluate the consistency of the mediation pathway across individual compliance sub-dimensions and conduct sensitivity analyses with alternative model specifications.

International Journal of Management Technology, 13(2), 73-90, 2026
Print ISSN: ISSN 2055-0847(Print)
Online ISSN: ISSN 2055-0855(Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

EXPECTED CONTRIBUTIONS OF THE STUDY

Theoretical Contributions

The study advances the theoretical literature in four ways. First, it contributes the first empirical integration of Protection Motivation Theory, General Deterrence Theory, and the Theory of Planned Behaviour within a single mediated model applied to cybersecurity policy compliance in a Nigerian federal dual-mode university, extending the reach of each paradigm beyond its predominant corporate and Western institutional settings. Second, by modelling cybersecurity awareness as a formal mediator between ISC and compliance, the study specifies the cognitive mechanism that has been theorised but rarely tested within the Nigerian higher education cybersecurity domain, contributing to the precision and explanatory completeness of behavioural compliance theory. Third, by operationalising ISC through CSETA a parsimonious, policy-actionable, and externally observable construct the study contributes a replicable measurement approach that can serve as a reference for subsequent African higher education cybersecurity research. Fourth, by treating CPC as a multi-dimensional construct encompassing IRB, DHP, and ITC, the study extends the construct's operationalisation beyond the unitary compliance intention measures that dominate the prior literature, enriching the theoretical understanding of how cultural interventions differentially shape distinct compliance domains.

Practical Contributions

Practically, the study provides Chief Information Security Officers, ICT directors, and security awareness coordinators in Nigerian federal universities with evidence on the relative contribution of CSETA to each compliance sub-dimension, enabling the prioritisation of training content, modality, and frequency for maximum behavioural impact. For institutional governance bodies including the Governing Council, Senate, and ICT Directorate of the University of Abuja the findings will support evidence-based calibration of cybersecurity policies, allocation of awareness programme budgets, and design of culture-shaping interventions. The explicit inclusion of students within the sample provides an inclusive evidence base that reflects the true composition of the university's ICT user community and supports the development of differentiated awareness strategies for staff and students respectively.

Policy Implications

At the national level, the findings will inform the guidance frameworks of the National Information Technology Development Agency, the Nigeria Data Protection Commission, and the National Universities Commission for higher education cybersecurity governance. By demonstrating which behavioural mechanisms are most responsive to CSETA investments within a federal dual-mode university, the study provides an empirical basis for refining the Cybercrimes Act compliance requirements and the National Cybersecurity Policy and Strategy directives as they apply to the tertiary education sector. The study also supports the development of sectoral implementation guidelines for the Nigeria Data Protection Act (2023), particularly in respect of the data-handling and protection obligations it imposes on educational institutions.

Contributions to the Field

The study makes several contributions to the broader field of cybersecurity behavioural research. It advances the methodological practice of the Nigerian higher education cybersecurity literature by deploying the Hayes (2022) PROCESS Macro Model 4 with bias-corrected bootstrap confidence intervals, providing a replicable template that supersedes the legacy Baron and Kenny (1986) causal-step procedure. It enriches the comparative basis for cross-institutional and cross-cultural cybersecurity research by adding a stratified dual-population (staff and student) evidence base from a Nigerian federal dual-mode university. Finally, it contributes a reference benchmark of construct validity and reliability statistics, instrument adaptation pathways, and sampling procedures for use by subsequent investigators working within Nigerian university or public sector settings.

CONCLUSION

This paper has presented the conceptual, theoretical, empirical, and methodological foundations for a study of the effect of Information Security Culture on Cybersecurity Policy Compliance in the University of Abuja, with Cybersecurity Awareness as a mediating variable. The study addresses a convergence of institutional, national, and scholarly imperatives. At the institutional level, the University of Abuja's dual-mode structure, heterogeneous user community, and positioning within Nigeria's evolving cybersecurity regulatory landscape create an acute need for evidence-based guidance on how cultural and cognitive mechanisms shape the security compliance behaviour of staff and students. At the national level, the persistence of human-mediated cybersecurity incidents despite significant regulatory advances underscores the inadequacy of technical controls alone and mandates systematic empirical investigation of the behavioural antecedents of compliance within the federal university system. At the scholarly level, the study addresses six identified gaps in the prior literature — conceptual, theoretical, empirical, methodological, population-related, and practitioner-knowledge — that have collectively limited the transferability and precision of existing evidence to the Nigerian higher education cybersecurity context.

The proposed integrated theoretical framework, combining Protection Motivation Theory, General Deterrence Theory, and the Theory of Planned Behaviour within a single mediated model, provides a richer and more complete explanatory structure than any single theory considered in isolation. The cross-sectional quantitative design, stratified sample of 400 staff and students, validated 33-item questionnaire, and application of the Hayes (2022) PROCESS Macro Model 4 with bias-corrected bootstrap confidence intervals together constitute a methodologically rigorous and replicable research design. The expected findings will quantify the direct effects of CSETA on Incident Response Behaviour, Data Handling and Protection, and Intention to Comply with Security Policies, as well as the indirect effect of CSETA on the composite compliance outcome through the mediating pathway of cybersecurity awareness. These contributions are expected to

advance theoretical integration, enrich the empirical evidence base for Nigerian higher education cybersecurity, and provide actionable guidance for institutional and national policy.

REFERENCES

African Union. (2014). African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). African Union.

Ahamed, B., Polas, M. R. H., Kabir, A. I., Sohel-Uz-Zaman, A. S. M., Al Fahad, A., Chowdhury, S., & Dey, M. R. (2024). Empowering students for cybersecurity awareness management in the emerging digital era: The role of cybersecurity attitude in the 4.0 industrial revolution era. SAGE Open, 14(1). https://doi.org/10.1177/21582440241228920

Aigbefo, Q. A., Blount, Y., & Marrone, M. (2022). The influence of hardiness and habit on security behaviour intention. Behaviour & Information Technology, 41(6), 1151–1170. https://doi.org/10.1080/0144929X.2020.1856928

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Alam, S. S., Ahsan, N., Kokash, H. A., Alam, S., & Ahmed, S. (2024). A students' behaviors in information security: Extension of Protection Motivation Theory (PMT). Information Security Journal: A Global Perspective, 34(3), 191–213. https://doi.org/10.1080/19393555.2024.2408264

Alraja, M. N., Butt, U. J., & Abbod, M. (2023). Information security policies compliance in a global setting: An employee's perspective. Computers & Security, 129, 103208. https://doi.org/10.1016/j.cose.2023.103208

Alrawhani, E. M., Romli, A. B., Al-Sharafi, M. A., & Alkawsi, G. (2025). Integrating information security culture and protection motivation to enhance compliance with information security policies in banking: Evidence from PLS-SEM and fsQCA. International Journal of Human–Computer Interaction, 41(20), 12728–12749. https://doi.org/10.1080/10447318.2025.2464900

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. MIS Quarterly, 34(3), 613–643. https://doi.org/10.2307/25750694

Arif, M., Badila, M., Warden, J. M., & Rehman, A. U. (2025). A study of human factors toward compliance with organization's information security policy. Information Security Journal: A Global Perspective, 34(3). https://doi.org/10.1080/19393555.2025.2457702

Baron, R. M., & Kenny, D. A. (1986). The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. Journal of Personality and Social Psychology, 51(6), 1173–1182. https://doi.org/10.1037/0022-3514.51.6.1173

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. MIS Quarterly, 39(4), 837–864. https://doi.org/10.25300/MISQ/2015/39.4.5

Bryman, A. (2016). Social research methods (5th ed.). Oxford University Press.

Bulgurcu, B., Cavusoglu, 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. https://doi.org/10.2307/25750690

Cochran, W. G. (1977). Sampling techniques (3rd ed.). John Wiley & Sons.

Cohen, J. (1988). Statistical power analysis for the behavioral sciences (2nd ed.). Lawrence Erlbaum Associates.

Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. MIS Quarterly, 43(2), 525–554. https://doi.org/10.25300/MISQ/2019/15117

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

Cyber Security Experts Association of Nigeria. (2023). Nigerian cybersecurity industry report 2023. CSEAN.

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. Computers & Security, 29(2), 196–207. https://doi.org/10.1016/j.cose.2009.09.002

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture: Perspectives from academia and industry. Computers & Security, 92, 101713. https://doi.org/10.1016/j.cose.2020.101713

Federal Ministry of Health. (2007). National code of health research ethics. Federal Ministry of Health, Nigeria.

Federal Republic of Nigeria. (2015). Cybercrimes (Prohibition, Prevention, etc.) Act, 2015. Government Printer.

Federal Republic of Nigeria. (2023). Nigeria Data Protection Act, 2023. Government Printer.

Federal Republic of Nigeria. (2024). Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024. Government Printer.

Field, A. (2018). Discovering statistics using IBM SPSS Statistics (5th ed.). SAGE Publications.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research, 18(1), 39–50. https://doi.org/10.1177/002224378101800104

Gibbs, J. P. (1975). Crime, punishment, and deterrence. Elsevier.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). Multivariate data analysis (8th ed.). Cengage Learning.

Han, M., Zhao, H., Ma, X., & Shi, R. (2025). Influencing factors of information security behavior among college students based on protection motivation theory: Evidence from China. Frontiers in Public Health, 13, 1677024. https://doi.org/10.3389/fpubh.2025.1677024

Hassandoust, F., Subasinghage, M., & Johnston, A. C. (2022). A neo-institutional perspective on the establishment of information security knowledge sharing practices. Information & Management, 59(1), 103574. https://doi.org/10.1016/j.im.2021.103574

Hayes, A. F. (2022). Introduction to mediation, moderation, and conditional process analysis: A regression-based approach (3rd ed.). The Guilford Press.

Hengstler, S., Kuehnel, S., Masuch, K., Nastjuk, I., & Trang, S. T.-N. (2023). Should I really do that? Using quantile regression to examine the impact of sanctions on information security policy compliance behavior. Computers & Security, 133, 103370. https://doi.org/10.1016/j.cose.2023.103370

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. Journal of the Academy of Marketing Science, 43(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8

Hong, Y., & Furnell, S. (2022). Motivating information security policy compliance: Insights from perceived organizational formalization. Journal of Computer Information Systems, 62(1), 19–28. https://doi.org/10.1080/08874417.2019.1683781

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. Structural Equation Modeling, 6(1), 1–55. https://doi.org/10.1080/10705519909540118

IBM Security. (2024). Cost of a data breach report 2024. IBM Corporation.

International Organization for Standardization, & International Electrotechnical Commission. (2018). ISO/IEC 27000:2018. Information technology—Security techniques—Information security management systems—Overview and vocabulary. ISO.

INTERPOL. (2024). African cyberthreat assessment report 2024. International Criminal Police Organization.

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. Educational and Psychological Measurement, 30(3), 607–610. https://doi.org/10.1177/001316447003000308

Lawshe, C. H. (1975). A quantitative approach to content validity. Personnel Psychology, 28(4), 563–575. https://doi.org/10.1111/j.1744-6570.1975.tb01393.x

Mou, J., Cohen, J. F., Bhattacherjee, A., & Kim, J. (2022). A test of protection motivation theory in the information security literature: A meta-analytic structural equation modeling approach. Journal of the Association for Information Systems, 23(1), 196–236. https://doi.org/10.17705/1jais.00723

National Information Technology Development Agency. (2021). National cybersecurity policy and strategy. NITDA.

National Information Technology Development Agency. (2022). Annual report. NITDA.

National Institute of Standards and Technology. (2003). NIST Special Publication 800-50: Building an information technology security awareness and training program. U.S. Department of Commerce.

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018

Neri, M., Benevento, E., Stefanini, A., Aloini, D., Niccolini, F., Carducci, A., Federigi, I., & Dini, G. (2025). Understanding information security awareness: Evidence from the public healthcare sector. Information and Computer Security, 33(3), 309–319. https://doi.org/10.1108/ICS-04-2024-0094

Nigerian Communications Commission. (2024). Industry statistics. NCC. https://www.ncc.gov.ng/statistics-reports/industry-overview

Nunnally, J. C. (1978). Psychometric theory (2nd ed.). McGraw-Hill.

Oroni, C. Z., Xianping, F., Ndunguru, D. D., & Ani, A. (2025). Enhancing cyber safety in e-learning environment through cybersecurity awareness and information security compliance: PLS-SEM and FsQCA analysis. Computers & Security, 150, 104276. https://doi.org/10.1016/j.cose.2024.104276

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. Journal of Applied Psychology, 88(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879

Polit, D. F., & Beck, C. T. (2006). The content validity index: Are you sure you know what's being reported? Critique and recommendations. Research in Nursing & Health, 29(5), 489–497. https://doi.org/10.1002/nur.20147

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. MIS Quarterly, 37(4), 1189–1210. https://doi.org/10.25300/MISQ/2013/37.4.09

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

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Eds.), Social psychophysiology: A sourcebook (pp. 153–176). Guilford Press.

Saunders, M., Lewis, P., & Thornhill, A. (2019). Research methods for business students (8th ed.). Pearson Education.

Straub, D. W. (1990). Effective IS security: An empirical study. Information Systems Research, 1(3), 255–276. https://doi.org/10.1287/isre.1.3.255

Tabachnick, B. G., & Fidell, L. S. (2019). Using multivariate statistics (7th ed.). Pearson Education.

Tran, D. V., Nguyen, P. V., Le, L. P., & Nguyen, S. T. N. (2025). From awareness to behaviour: Understanding cybersecurity compliance in Vietnam. International Journal of Organizational Analysis, 33(1), 209–229. https://doi.org/10.1108/IJOA-12-2023-4147

Tran, D. V., Nguyen, P. V., Vrontis, D., Nguyen, S. T. N., & Dinh, P. U. (2024). Unraveling influential factors shaping employee cybersecurity behaviors: An empirical investigation of public servants in Vietnam. Journal of Asia Business Studies, 18(6), 1445–1464. https://doi.org/10.1108/JABS-01-2024-0058

United States Department of Health, Education, and Welfare. (1979). The Belmont Report: Ethical principles and guidelines for the protection of human subjects of research. National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research.

University of Abuja. (n.d.). About us. University of Abuja. https://www.uniabuja.edu.ng/about-us

Verizon. (2024). 2024 data breach investigations report. Verizon Business.

World Medical Association. (2013). Declaration of Helsinki: Ethical principles for medical research involving human subjects. JAMA, 310(20), 2191–2194. https://doi.org/10.1001/jama.2013.281053

Yusif, S., & Hafeez-Baig, A. (2023). Cybersecurity policy compliance in higher education: A theoretical framework. Journal of Applied Security Research, 18(2), 267–288. https://doi.org/10.1080/19361610.2021.1989271