International Journal of Innovative Information Systems & Technology Research 13(4):399-412, Oct-Dec, 2025

 www.seahipublications.org ISSN: 2467-8562

doi:10.5281/zenodo.17918271

A Structural Assessment Model for Cybersecurity Policy Effectiveness

Nasir S. Yakubu[1], Monday O. Adenomon[2], & Francisca N. Ogwueleka[3]

[1, 2]Center for Cyberspace Studies, Nasarawa State University, Keffi, NIGERIA
[3]Department of Computer Science, University of Abuja, Abuja-FCT, NIGERIA

ABSTRACT

Effective cybersecurity policy remains a critical challenge for public-sector institutions, particularly in developing economies where gaps in policy design, implementation, and user compliance limit institutional readiness. This study develops a Structural Assessment Model for Cybersecurity Policy Effectiveness, integrating four constructs: Policy Design, Implementation Success, User Compliance, and Institutional Readiness. A quantitative cross-sectional design was employed with 72 respondents across three Nigerian public-sector institutions. Data were collected via a validated Likert-scale questionnaire and analysed using reliability testing, descriptive statistics, multiple regression, and a hybrid empirical weighting model (PCA–variance–regression, 40/30/30) for computing the Cybersecurity Policy Effectiveness Index (CPEI). Regression results indicate that Policy Design, Implementation Success, and User Compliance significantly predict Institutional Readiness ($R^2 = 0.857$, $p < 0.001$). The resulting CPEI score of 3.836 (76.72%) categorises the institutions as High Effectiveness. The study provides both theoretical and practical contributions by offering an integrated framework linking policy, implementation, and compliance to readiness, and by introducing a replicable CPEI tool for benchmarking organisational cybersecurity performance in resource-constrained environments.

Keywords*:* Cybersecurity Performance Index (CPEI), Data Protection Impact Assessments (DPIAs), Security Information and Event Management (SIEM), Intrusion Detection/Protection Systems (IDS/IPS), Protected Motivated Theory (PMT), Computer Security Incident Response Team (CSIRT).

1. INTRODUCTION

The rapid digitalisation of public services has heightened cybersecurity risks across government institutions, making effective cybersecurity governance essential for safeguarding national information assets. Although global frameworks such as ISO/IEC 27001 and the NIST Cybersecurity Framework provide structured guidance, their effectiveness depends on how well organisations adapt them to local institutional realities.

Despite having formal cybersecurity policies, many public-sector institutions, especially in developing economies, remain vulnerable to cyber incidents. Persistent weaknesses in policy design, inconsistent implementation, low user compliance, and limited institutional capacity prevent cybersecurity policies from achieving their intended outcomes.

Existing studies tend to examine policy design, implementation challenges, and user behaviour independently, resulting in fragmented insights. There is limited empirical evidence that integrates these

constructs into a single model capable of assessing how they collectively influence institutional readiness, particularly within the context of developing-country public institutions.

This study aims to develop and validate a Structural Assessment Model for Cybersecurity Policy Effectiveness that examines how Policy Design, Implementation Success, and User Compliance predict Institutional Readiness. It also introduces the Cybersecurity Policy Effectiveness Index (CPEI) as a composite measure of organisational cybersecurity maturity.

The study provides a unified assessment model, develops validated constructs tailored to public-sector contexts, and introduces the CPEI for quantifying cybersecurity policy effectiveness. It offers evidence-based insights to guide policymakers and cybersecurity managers in strengthening institutional governance, improving compliance culture, and enhancing national cyber readiness.

2. Review of Related Studies

2.1 Global Cybersecurity Frameworks and their Relevance to Public Institutions

International standards and frameworks provide the baseline vocabulary and control logic for organisational cybersecurity. ISO/IEC 27001 (2022) specifies requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS), positioning governance, risk management, and continual improvement as foundational elements for sustained security performance (ISO, 2022). The NIST Cybersecurity Framework (CSF) 2.0 similarly structures cybersecurity outcomes through core functions; Govern, Identify, Protect, Detect, Respond, and Recover, explicitly linking organisational governance to operational security activities (NIST, 2024). These frameworks are valuable because they translate cybersecurity from a purely technical problem into an organisational management problem; however, evidence from developing-country public institutions suggests that adoption often remains "formal" (policy on paper) rather than operational (policy in practice) when resources, skills, and institutional coordination are limited (IISS, 2023).

2.2 Control Prioritisation and Operational Translation: CIS Controls and Practical Implementation Constraints

While ISO/IEC 27001 and NIST CSF provide high-level management structures, the CIS Controls translate security governance into prioritized, actionable technical and operational safeguards. In practice, agencies in resource-constrained settings may struggle with prerequisites that the Controls assume; reliable asset inventories, enforceable configuration baselines, and consistent monitoring capacity, thereby creating implementation bottlenecks even when policy commitments exist (Ojuri, 2022). This tension between "what should be done" (standards) and "what can be done" (operational capacity) is central to understanding why policy effectiveness varies across institutions.

2.3 African and Nigerian Evidence: Contextual Drivers of Policy Effectiveness

Empirical work from Nigeria and broader African contexts highlights recurring constraints: fragmented national coordination, skills shortages, weak organisational resourcing, and uneven compliance cultures (IISS, 2023; Ojuri, 2022). Recent Nigerian studies further indicate that policy outputs; such as the National Cybersecurity Policy and Strategy and related legislative instruments, do not automatically translate into institutional readiness unless implementation mechanisms, enforcement, and workforce capability are strengthened (Adeleke et al., 2023; Cybersecurity Policy Implementation and Nigeria's Digital Positioning, 2025; An Interrogation of Nigeria's National Cyber Security Policy, 2025). These findings support the argument that effectiveness must be assessed through a combined lens of design quality, implementation performance, and user behaviour, rather than by mere policy existence.

2.4 From Determinants to Outcomes: Policy Design, Implementation Success, User Compliance, and Institutional Readiness

Across governance and implementation scholarship, policy outcomes are shaped by (a) the quality of the initial design (clarity, scope, accountability), (b) the success of implementation (resources, leadership support, monitoring), and (c) the behavioural response of users who operationalise or bypass security controls (Adeleke et al., 2023; Ojuri, 2022).

In this study, Policy Design captures the extent to which the policy is clearly structured, role-defined, standards-aligned, and supported by formal review mechanisms; Implementation Success captures the degree to which execution is supported by leadership, resources, and monitoring; User Compliance captures adherence and organisational security culture; and Institutional Readiness reflects the combined capacity to prevent, detect, respond to, and recover from cyber incidents (NIST, 2024; ISO, 2022).

2.5 Theoretical and Conceptual Anchoring (Towards a Structural Assessment Model)

To provide a coherent explanation for how these determinants interact, the study aligns with implementation theory, where policy outcomes depend on the fit between policy design and organisational capacity, and with technology governance perspectives that treat cyber risk management as an integrated socio-technical system (NIST, 2024; ISO, 2022). Building on this grounding, the paper proposes a Structural Assessment Model for Cybersecurity Policy Effectiveness in which Policy Design, Implementation Success, and User Compliance jointly predict Institutional Readiness (the operational outcome).

2.6 Conceptual Framework (Structural Assessment Model)

Figure 1: Conceptual framework Structural Assessment Model (SAM) (Source: Author)

Policy Design, Implementation Success, and User Compliance function as the core drivers of cybersecurity effectiveness. These three constructs jointly determine Institutional Readiness, the dependent variable. Institutional Readiness then feeds into the Cybersecurity Policy Effectiveness Index (CPEI), a composite output that rates the organisation's cybersecurity maturity. The model reflects both predictive pathways (regression-based) and structural logic (theoretical framework).

2.7 Literature Review Summary and Identified Gap

Although global frameworks (ISO/IEC 27001; NIST CSF 2.0) provide strong foundations, the Nigerian evidence base shows that adoption frequently remains uneven and organisation-specific (Adeleke et al., 2023; An Interrogation of Nigeria's National Cyber Security Policy, 2025). Existing studies tend to treat design, implementation, or compliance separately; what remains underdeveloped is an integrated, empirically tested model that links these determinants to institutional readiness and converts the result into a usable composite measure. This gap motivates the Structural Assessment Model and the Cybersecurity Policy Effectiveness Index (CPEI) developed in this study.

3. METHODOLOGY

3.1 Research Design

The research design serves as the blueprint for systematically collecting, analyzing and interpreting data to achieve the objectives of a study (Creswell, 2018). The assessment model adopted a mixed-methods approach, integrating both quantitative (questionnaires) and qualitative (interviews) data collection tools. These are applied across three complementary designs, namely: i) Descriptive Design: To document institutional cybersecurity practices, structures and compliance mechanisms, ii) Evaluative Design: To assess the effectiveness of existing policies using the Cybersecurity Policy Effectiveness Index (CPEI), and iii) Comparative Design: To identify variations and best practices across the selected institutions. Figure 2 showed the research design, the environmental context, research philosophy and research methodology adopted for this study. The framework visually mapped how data flows from respondents and institutions through these designs into a combined analysis, leading to a validated, context-specific model for measuring cybersecurity policy effectiveness in institutions.

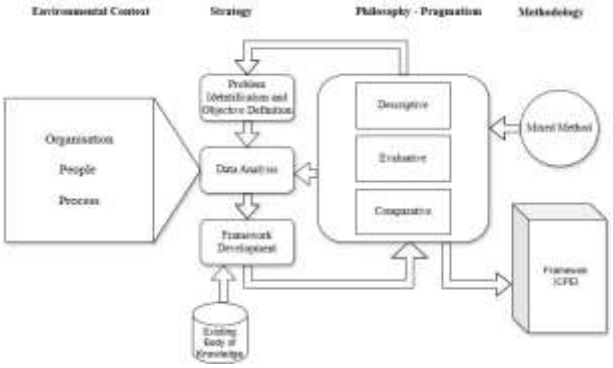

Figure 2: Conceptual Research Design Framework for the CPEF (Source: Author)

3.1.1 Environmental Context

The environmental context of this study referred to the socio-technical, regulatory and institutional ecosystem within which cybersecurity policies are designed, implemented and evaluated in institutions. When conducting a study, examine the phenomenon's context (Mbanaso et al., 2023). This entails examining the factors that can shape or establish the problem that is being addressed. Thus, this study focused around organisation, people and process. Typically, cybersecurity environment is characterised by evolving policies, constrained institutional capacities, diverse user behaviours and a growing need to align with international standards. This context framed the need for a well-designed, evidence-based policy framework that addresses not only process vulnerabilities but also institutional and human factors.

3.1.2 Strategy: Problem-Driven Research Process

The strategy phase comprises three stages: i) Problem Identification and Objective Definition: Informed by observed gaps in policy effectiveness and institutional practice, the research problem is defined in alignment with practical realities, ii) Data Analysis: Empirical data from questionnaires and interviews are analysed to assess the current state and performance of cybersecurity policies, and iii) Framework Development: Insights from data analysis and literature are synthesised to develop the Cybersecurity Policy Effectiveness Index (CPEI. The existing body of knowledge supported this entire process by offering relevant theories, models, and frameworks that are adapted to the study's context.

3.1.3 Philosophy: Pragmatism

Pragmatism was chosen for this study to address complex, real-world problem. Pragmatism supports the integration of multiple research designs, descriptive, evaluative and comparative: i) Descriptive Design: Identifies and documents current cybersecurity practices and structures, ii) Evaluative Design: Measures the effectiveness of cybersecurity policies, and iii) Comparative Design: Pragmatism also provides the flexibility to iterate between these stages and adjust the research design as needed to ensure both rigour and relevance

3.2 Population, Sampling, and Sample Size Justification

3.2.1 Population

The target population for this study includes personnels directly involved in cybersecurity governance and usage within organisations. This comprises of IT professionals (e.g., cybersecurity officers, system administrators), policy implementers and decision-makers (e.g., CIOs, compliance officers) and end-users of cybersecurity policies (e.g., staff in government or private institutions). These participants would be selected from Government, Private, Regulatory or Professional and Academic Institutions engaged in digital operations and cybersecurity governance.

3.2.2 Sample Size

In determining the sample size for the quantitative aspect of this study, Yamane's (1967) formula for a finite population was applied. This formula provides a simplified approach to calculate the minimum sample size required to achieve a desired level of precision within a given population size. The population with the desired characteristics of being involved in the survey was considered 5% and the margin of error to be 10%.

$$n = \frac{N}{1+N(e)^2} \quad (3.1)$$

Where:
n = required sample size
N = population size (10,000)
e = margin of error (0.1) or precision

$$n = \frac{10,000}{1+10,000(0.1)^2}$$
$$n = \frac{10,000}{1+10,000(0.01)}$$
$$n = \frac{10,000}{1+100}$$
$$n = \frac{10,000}{101} \approx 99.01$$

With a population of 10,000 and a margin of error of 10%, a sample size of approximately 99 respondents is sufficient to achieve statistically meaningful results in this study. Although this study utilised a sample size of 100 respondents for the quantitative phase and 10 interviewees for the qualitative phase, limitations exist in terms of statistical generalizability, potential nonresponse bias, and constraints in conducting advanced multivariate analysis.

3.2.2 Sampling Techniques

The study will use a stratified purposive sampling approach. Participants are deliberately selected based on relevance to the research objective. Stratification ensures representation across relevant categories (e.g. sector, role, experience level). Purposive sampling allows selection of individuals who have first-hand knowledge of cybersecurity policies and practices (Palinkas et al., 2015). This approach supports the mixed methods design by ensuring that both quantitative breadth and qualitative depth are captured.

3.3 Methods of Data Collection

The study applied data collection framework designed for a mixed-methods research study, particularly in the context of cybersecurity policy effectiveness. It integrated quantitative, qualitative and documentary data sources, organised within data collection framework.

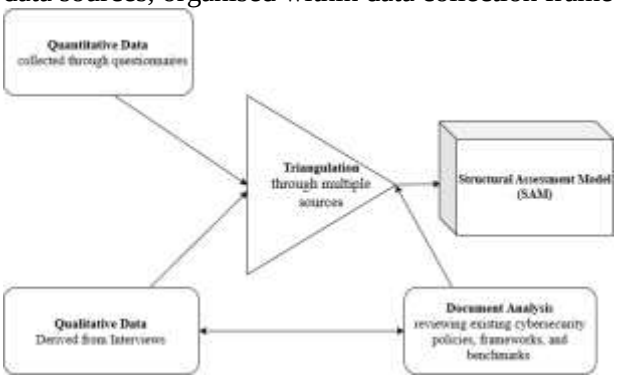

Figure 3: Data Collection for the SAM (Source: Author)

In this study, the respondents were selected from four critical sectors that have responsibility for implementing cybersecurity policies to protect critical infrastructure (CI). The participants will include Government, Private Institutions, Regulatory Institutions and Professional Bodies, and Academic Institutions where structured questionnaires and semis-structured interviews will be conducted.

Table 1: Distribution of Quantitative Data Sources and Target Audiences (n = 100)

Institution / Department	Target Audience	Estimated Respondents
Government – Public Sector Institutions – IT, Admin / HR Departments	Cybersecurity Staff, IT Managers, HR Officers, Policy Admins	**60**
Private Institutions – IT, Admin / HR Departments	Cybersecurity Staff, IT Managers, HR Officers, Policy Admins	**20**
Regulatory Institutions IT, Admin / HR Departments	Cybersecurity Staff, IT Managers, HR Officers, Policy Admins	**10**
Academic Institutions – IT, Admin / HR Departments	Cybersecurity Staff, IT Managers, HR Officers, Policy Admins	**10**
Total		**100**

In this study, the qualitative data were collected using semi-structured interviews, where participants with shared roles (e.g., IT or policy managers) were engaged in guided proving insights (Insight7., 2024). Participants were engaged based on the distribution depicted in Table 3.

Table 2: Distribution of Quantitative Data Sources and Target Audiences (n = 10)

Institution / Department	Target Audience	Estimated Respondents
Government – Public Sector Institutions – IT, Admin / HR Departments	Cybersecurity Staff, IT Managers, HR Officers, Policy Admins	**6**
Private Institutions – IT, Admin / HR Departments	Cybersecurity Staff, IT Managers, HR Officers, Policy Admins	**2**
Regulatory Institutions IT, Admin / HR Departments	Cybersecurity Staff, IT Managers, HR Officers, Policy Admins	**1**
Academic Institutions – IT, Admin / HR Departments	Cybersecurity Staff, IT Managers, HR Officers, Policy Admins	**1**
Total		**10**

The semi-structured format provided a flexible guide of open-ended questions while allowing participants the freedom to introduce issues they considered important, ensuring accurate information/perception in both structure and depth. The group size was intentionally kept small to facilitate active participation and rich thematic discussion.

3.3.1 Triangulation

Data from all three sources are integrated and compared to ensure validity, comprehensiveness and consistency in the findings. Leveraging human factors in cybersecurity, an integrated approach and research agenda (Pollini et al., 2021). This is especially critical in triangulation, where design, demonstration and evaluation must be informed by multiple, corroborated perspectives.

3.3.2 Justification Method

The quantitative method employed to statistically test relationships among key variables (e.g., policy design, implementation, compliance, and institutional support), while the qualitative method provides depth by exploring underlying reasons, perceptions, and institutional dynamics through semi-structure interviews. The integration of both strands ensures methodological triangulation, enhancing the validity and reliability of the findings and contributing to a more robust policy effectiveness framework.

3.3.3 Reliability and Validity

Cronbach's Alpha was computed for all constructs to assess internal consistency. The results exceeded the 0.7 threshold (Ahmad et al., 2024), confirming acceptable reliability:

Table 3: Reliability and Validity of the Constructs

Constructs	**α**
Policy Design	0.797
Implementation Success	0.911
User Compliance	0.924
Institutional Readiness	0.848

Policy design recorded a cronbach's alpha of 0.797, indicating satisfactory internal consistency among the indicators measuring clarity, adequacy, and applicability of cybersecurity policy frameworks. Implementation success (α = 0.911) and user compliance (α = 0.924) showed excellent reliability, suggesting strong inter-item correlation and a coherent measurement of their respective constructs. Likewise, institutional readiness (α = 0.848) reflected high reliability, confirming that the indicators used to assess organisational preparedness and leadership support were consistent and dependable.

3.4 Ethical Considerations

In order not to coerce participants were provided with details about the study's objectives, procedures and their rights before giving their consent. Participation was also voluntary and consensual informing respondents could withdraw at any stage without consequences or breach of agreement. Identity of participants were anonymised, such that no personally identifiable information was collected. Secured data storage medium with password-protected mechanism was used, in compliance with the General Data Protection Regulation (GDPR) and the Nigeria Data Protection Regulation (NDPR), and will be securely deleted after the study. The study was designed to avoid physical, psychological or reputational harm or damage to participants. The findings are reported truthfully and without misrepresentation.

4. Development of the Structural Assessment Model (SAM)

Data were collected using a structured questionnaire with five-point Likert-scale items (1 = Strongly Disagree; 5 = Strongly Agree). Items for each construct were adapted from established frameworks and contextualised to Nigerian public-sector realities: - Policy Design: clarity of documentation, role/accountability definition, standards alignment (ISO/IEC 27001; NIST CSF), scope coverage, and formal review/version control (ISO, 2022; NIST, 2024). - Implementation Success: leadership commitment, resourcing, training and awareness, enforcement/monitoring, and incident response operationalisation (NIST, 2024; Adeleke et al., 2023). - User Compliance: adherence to access controls, acceptable-use practices, reporting behaviour, and follow-through on security procedures (Ojuri, 2022). - Institutional Readiness (DV): perceived capacity to prevent, detect, respond to, and recover from cyber incidents (NIST, 2024).

4.1 Data Analysis and Regression Model

Data analysis proceeded in three stages: (1) descriptive statistics (means, standard deviations, range) to profile responses; (2) computation of composite scores for each construct by averaging its items; and (3) multiple linear regression with Institutional Readiness as the dependent variable and Policy Design, Implementation Success, and User Compliance as predictors. Model adequacy was evaluated using R^2, adjusted R^2, F-statistics, and residual standard error.

4.1.1 Regression Model Specification

To understand how each construct contributes to overall cybersecurity maturity, a multiple regression model was estimated with Institutional Readiness as the dependent variable (DV) and three predictors:

i. Policy Design (PD)
ii. Implementation Success (IS)
iii. User Compliance (UC)

The model is expressed as:

$$IR = \beta_0 + \beta_1 PD + \beta_2 IS + \beta_3 UC + \varepsilon \qquad (4.1)$$

Where:
IR= Institutional Readiness
$\beta_1, \beta_2, \beta_3$= estimated influence of each construct
ε= error term
Based on the actual data (N = 72), the regression yielded:

Table 4: Regression Output (Source: Field Survey, 2025)

Statistic	Value
R^2	0.857
Adjusted R^2	0.849
F-statistic	100.52, $p < 0.001$
Residual SE	0.424

The three constructs jointly explain 85.7% of the variation in Institutional Readiness; a very strong model. All predictors significantly contribute to cybersecurity maturity. This confirmed that Institutional Readiness is a valid dependent construct for explaining cybersecurity effectiveness.

4.1.2 Descriptive Statistics

The core constructs of the study were measured on a 5-point Likert scale (1=Strongly Disagree, 5=Strongly Agree). The results are summarised in Table 5.

Table 5: Descriptive Statistics of Key Variables (n=72) (Source: Field Survey, 2025)

Variable	Mean	Standard Deviation	Min	Max
Policy Design	4.069	0.888	1.0	5.0
Implementation Success	3.903	0.815	1.0	5.0
User Compliance	3.653	0.925	1.0	5.0
Institutional Readiness	3.792	0.921	1.0	5.0

The findings show that Policy Design, Implementation Success, and User Compliance significantly influence Institutional Readiness. Policy Design is the strongest predictor, affirming that structured, clear, and adaptable policies are foundational for cybersecurity maturity. Implementation Success indicates that even well-crafted policies require practical leadership support and adequate resourcing to succeed. User Compliance further reinforces that human behaviour is a critical component of cybersecurity readiness.

4.1.3 Computation of the Composite Score (CPEI)

Step 1: What the CPEI Represents: The Cybersecurity Policy Effectiveness Index (CPEI) is a composite measure that combined the mean performance of the four key constructs in this model: i) Policy Design (PD), ii) Implementation Success (IS), iii) User Compliance (UC), iv) Institutional Readiness (IR). It reflected how effectively cybersecurity policies are designed, implemented, complied with, and supported institutionally, summarised into a single index value:

Step 2: Data Inputs for the CPEI Calculation: Each construct's mean (M_i) was calculated from the average of its related survey items.

In this study, an average of the mean of each construct was computed: a) mean of PD, b) mean of IS, c) mean of UC, d) mean of IR.

Step 3: How the Weights Were Derived (Hybrid 40/30/30 Model): Principal Component Analysis (PCA) was employed in this study to determine the statistical contribution and dimensional strength of each construct: Policy Design, Implementation Success, User Compliance, and Institutional Readiness, to overall cybersecurity policy effectiveness. The first principal component (PC1) was extracted, as it accounted for the largest proportion of total variance (above 70%), indicating that a single composite factor underlies the four constructs. The component loadings of each construct on PC1 represented their statistical contribution to the overall model and served as the basis for 40% of the CPEI weighting scheme.

This approach ensured that constructs with stronger structural relationships (higher loadings on PC1) received greater influence in the final index computation. The use of PCA thus enhanced the objectivity and robustness of the CPEI by grounding the weighting process in empirical data rather than arbitrary

assumptions. Then, each construct was assigned a final weight (w_i) using Principal Component Analysis (PCA), with hybrid weighting model (40/30/30). Each construct's weight (w_i) was calculated from three components:

$$w_i = 0.40 \mid L_i \mid +0.30V_i + 0.30 \mid r_i \mid \quad (4.1)$$

Where:

$\mid L_i \mid$ = Absolute PCA Loading of construct i on PC1. This shows the structural contribution of the construct.

V_i = Normalised Variance Share of construct i. This is obtained by squaring loadings and normalising them across constructs.

$\mid r_i \mid$ = Absolute Correlation between the construct and Policy Effectiveness (DV). This captures the empirical linkage between the construct and the dependent variable. These three elements were normalised so that the total weight equals 1.00 (or 100%). Using the formula above, the hybrid model produced four raw weights:

Table 6: Weights Scores for the Constructs (Source: Field Survey, 2025)

Construct	Raw Weight (w_i)
Policy Design	0.532
Implementation Success	0.739
User Compliance	0.764
Institutional Readiness	0.754

These raw weights cannot be used directly, because they do not sum to 1. To make them meaningful in an index, they must be normalised to sum to **1 (or 100%)**, making the index mathematically interpretable.
The formula for normalisation is:

$$W_i = \frac{w_i}{\sum w_i} \quad (4.2)$$

Using the formula for normalisation above:

$$\sum w_i = 0.532 + 0.739 + 0.764 + 0.754 = 2.789$$

Then each weight is divided by 2.789:

Table 7: Normalised weights for the Constructs

Construct	Normalised Weight (W_i)
Policy Design	0.191
Implementation Success	0.265
User Compliance	0.274
Institutional Readiness	0.270

The weights were derived empirically from PCA loadings, variance explained, and regression coefficients using a 40/30/30 hybrid formula, and then normalised so that they sum to 1, resulting in the final weights (0.191, 0.265, 0.274, 0.270) used in the CPEI computation.

Step 4: Applying the Weights to Compute CPEI: The CPEI is computed as a weighted average of the mean scores of the four constructs:

$$CPEI = \frac{\sum_{i=1}^{n} w_i \times M_i}{\sum_{i=1}^{n} w_i} \quad (4.3)$$

Where:
Mi = Mean score of constructs i
wi = Weight assigned to construct i
n = Number of constructs (here, 4)
Thus, the CPEI was computed:

$$CPEI = (0.191 \times 4.069) + (0.265 \times 3.903) + (0.274 \times 3.653) + (0.270 \times 3.792)$$

Since the sum of weights = 1, this simplifies to:

CPEI=0.777+1.034+1.001+1.024 ≈ 3.836.

The computed CPEI = 3.836 represents the overall cybersecurity policy effectiveness level on a 5-point scale, this corresponds to 76.72% categorised as high effectiveness, indicating mature policy design, implementation, and institutional readiness across the participating organisations.

5. FINDINGS AND DISCUSSION OF THE RESULTS

The findings show that Policy Design, Implementation Success, and User Compliance significantly influence Institutional Readiness. Policy Design is the strongest predictor, affirming that structured, clear, and adaptable policies are foundational for cybersecurity maturity. Implementation Success indicates that even well-crafted policies require practical leadership support and adequate resourcing to succeed. User Compliance further reinforces that human behaviour is a critical component of cybersecurity readiness.

The CPEI categorisation demonstrates that the assessed organisations exhibit High Effectiveness, though opportunities exist for strengthening compliance culture and improving execution processes.

The descriptive statistics showed a mean rating of 4.069 on policy design clarity, suggesting moderately high agreement among participants. User compliance had a lower average (mean = 3.653), indicating gaps in routine adherence to cybersecurity protocols. Implementation support mechanisms, such as training and technical assistance, scored moderately high across institutions with a mean rating of 3.903.

All constructs recorded mean values above 3.50, indicating positive institutional performance across the key dimensions of cybersecurity governance. policy design (M = 4.069) achieved the highest mean, suggesting that cybersecurity policies within the sampled institutions are perceived as well-structured, coherent, and clearly communicated. implementation success (M = 3.903) followed closely, reflecting that organisations generally execute their cybersecurity strategies effectively. user compliance (M = 3.653) and institutional readiness (M = 3.792) also exhibited strong mean values, signifying that both employee adherence and organisational support systems play significant roles in policy success.

These findings affirmed that policy effectiveness can be systematically measured through multi-dimensional assessment frameworks, such as the Cybersecurity Policy Effectiveness Index (CPEI), which integrated design quality, implementation capacity, compliance behaviour, and institutional readiness into a composite performance score.

5. Contributions of the Study

The findings of this study contributed significantly to the growing body of literature on cybersecurity policy effectiveness by integrating both quantitative measures and qualitative insights into a unified analytical framework. Empirically, the study makes three critical contributions:

i) Development of the Cybersecurity Policy Effectiveness Index (CPEI): A novel quantitative composite measure that aggregates policy design, implementation, compliance, and readiness into a single diagnostic index.

ii) The CPEI model thus provided both policymakers and institutional leaders with a contextually adaptive and empirically verifiable tool for continuous cybersecurity performance improvement.

iii) This model extended previous frameworks by moving beyond isolated maturity or compliance assessments to an evidence-based evaluation model linking technical capability, institutional governance, and human behaviour.

6. CONCLUSION

The study concluded that cybersecurity policy effectiveness depends on both institutional systems and human behaviour. While some institutions have made commendable progress in policy design and implementation, gaps remain in user compliance, readiness, and continuous monitoring.

The CPEI underscored that some institutions are on a trajectory toward higher maturity, but sustained improvements in behavioural compliance and institutional readiness are necessary to reach transformative levels.

The CPEI framework therefore bridged the gap between cybersecurity policy formulation and measurable outcomes, showing that effectiveness cannot be determined by documentation alone but by how well policies are internalised, enforced, and sustained.

Theoretically, the research validated Design Science Research (DSR) and Diffusion of Innovation (DOI) as relevant lenses for cybersecurity policy studies, demonstrating that adoption, adaptation, and continuous improvement are integral to achieving policy success.

7. RECOMMENDATIONS

Based on the research findings and conclusions, the following recommendations are made:

i) Institutionalise the Cybersecurity Policy Effectiveness Index (CPEI): All public and private sector institutions should adopt the CPEI as a standard evaluation tool to measure, compare, and improve cybersecurity performance using the indices.

ii) Strengthen Governance and Leadership Accountability: Cybersecurity objectives should be incorporated into executive scorecards, with management held accountable for compliance, training, and incident response outcomes.

iii) Foster Behavioural Change and Awareness: Institutions should implement continuous security awareness programs, tailored to user behaviour and embedded within human resources (HR) and performance management systems (PMS).

iv) Integrate CPEI Metrics into Organisational Dashboards: Use CPEI-based dashboards to track progress, generate periodic reports, and support evidence-driven decision-making at both institutional and national levels.

v) Enhance Multi-Stakeholder Collaboration: Regulators such as NITDA, NCC, and ONSA should coordinate unified cybersecurity measurement templates and offer regular benchmarking workshops across sectors.

vi) Periodic Policy Review and Adaptation: Conduct annual policy audits to align with emerging technologies, risks, and the evolving national priorities like the Nigeria's National Digital Economy Policy and Strategy (NDEPS).

8. Limitations of the Study

While the study achieved its objectives, certain limitations should be noted:

i) Sample Size and Institutional Representation: The study involved 72 respondents across some CNI institutions, which may not fully represent Nigeria's diverse cybersecurity landscape. To minimise sampling bias, the selected institutions were drawn from 3 critical national infrastructure (CNI) sectors representing government, education, and service delivery. The multi-method design (survey and interview) also provided triangulated evidence, improving the depth and representativeness of findings.

ii) Cross-Sectional Design: Data were collected at a single point in time, limiting the ability to observe longitudinal changes in policy implementation or compliance behaviour. The study embedded temporal indicators (e.g., duration of policy adoption and frequency of updates) within survey items and interview prompts, allowing inference of maturity trends.

iii) Self-Reported Data: Survey and interview responses were based on participants' perceptions, which may introduce subjectivity or social-desirability bias. Multiple validity checks were applied: a) Cronbach's Alpha (0.797–0.924) confirmed internal consistency, b) data triangulation between quantitative and qualitative results reduced bias, and c) anonymised participation encouraged honest responses.

iv) Restricted Access to Sensitive Data: Confidentiality concerns limited access to internal audit and incident reports, which might have offered deeper technical validation of results. The study relied on proxy indicators such as institutional readiness, audit frequency, and policy implementation evidence, which were validated through expert interviews.

9. Suggestions for Further Research

To build upon this research, future scholars should consider:

i) Longitudinal Assessment: Apply the CPEI framework over several years to monitor institutional progress and policy sustainability.

ii) Sector-Specific Adaptations: Tailor and validate the framework across sectors such as finance, education, energy, and healthcare.

iii) Integration of Artificial Intelligence (AI) and Machine Learning (ML): Explore the use of AI and ML to automate real-time compliance tracking and policy evaluation.

iv) Cross-National Benchmarking: Compare Nigeria's CPEI results with other African countries to develop a Regional Cybersecurity Effectiveness Index.

REFERENCES

Adeleke, O., Onifade, A., & Ogunleye, A. (2023). *Cybersecurity policy implementation in Nigeria: Challenges and opportunities*. *Journal of Cyber Policy and Governance, 5*(1), 34–48.

Ahmad, N., Alias, F. A., Hamat, M., & Mohamed, S. A. (2024). Reliability analysis: application of cronbach's alpha in research instruments. *Pioneering the Future: Delving Into E-Learning's Landscape*, 114-119.

Akinjobi, T., Bello, S., & Alao, I. (2021). Assessing cybersecurity policy implementation in Nigerian public institutions. Journal of Information Security and Cybercrime Research, 5(2), 44–60.

Al-Mutairi, F., & Haddad, R. (2024). Exploring reasons for cybersecurity non-compliance in municipal governments in the UAE and Jordan. Journal of Information Security Policy, 19(1), 55–72.

Alshaikh, M. (2020). Developing cybersecurity policy and strategy for organisations: The need for a holistic approach. Information and Computer Security, 28(1), 1–14. https://doi.org/10.1108/ICS-04-2019-0044.

Awad, A., Hassan, M., & Youssef, A. (2023). Validating the Unified Model of Information Security Policies Compliance (UMISPC). Information Security Journal: A Global Perspective, 32(3), 201–215.

Center for Internet Security (CIS). (2021). CIS Controls v8 – The 18 Critical Security Controls. Retrieved from https://www.cisecurity.org/controls/cis-controls-list.

Daniels, O. (2023). National Cybersecurity Policy and Strategy of Nigeria: A Case Study (Doctoral dissertation, Capitol Technology University). ProQuest Dissertations & Theses, Order No. 30527879.

European Union Agency for Cybersecurity (ENISA). (2022). Cybersecurity resilience maturity measurement (CRMM) framework. https://www.enisa.europa.eu/publications/crmm.

Federal Government of Nigeria. (2021). National Cybersecurity Policy & Strategy (NCPS). Abuja, Nigeria: Office of the National Security Adviser. Retrieved from https://cert.gov.ng/ngcert/resources/NATIONAL_CYBERSECURITY_POLICY_AND_STRATEGY_2021.pdf.

Garba, A. A., Siraj, M. M., & Othman, S. H. (2020). An Explanatory Review on Cybersecurity Capability Maturity Models. ASTES Journal, 6(3), 41-56. Retrieved from https://www.researchgate.net/publication/343932963_An_Explanatory_Review_on_Cybersecurity_Capability_Maturity_Models.

Heeks, R., & Bailur, S. (2007). Analyzing e-government research: Perspectives, philosophies, theories, methods, and practice. Government Information Quarterly, 24(2), 243–265.

International Institute for Strategic Studies (IISS). (2023). Cyber capabilities and national power: Nigeria (Vol. 2). https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/09/cyber-capabilities-and-national-power-vol-2/cyber-capabilities-and-national-power_volume-2_08-nigeria.pdf.

International Telecommunication Union. (2021). Global Cybersecurity Index 2020 (42 pages). Geneva: ITU. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

International Telecommunication Union. (2022). Decisions and Resolutions, Final Acts of the Plenipotentiary Conference (PP-22, Bucharest, 2022). Geneva: ITU.

Insight7. (2024). Qualitative research methods for IT policy analysis. Insight7 Research Reports. Retrieved from https://insight7.io/comprehensive-list-of-qualitative-research-methods-for-2024.

ISACA. (2019). COBIT 2019 Framework: Governance & Management Objectives. ISACA. https://www.isaca.org/resources/cobit.

Mbanaso, U. M., Abayomi, A., & Ndukwe, C. (2023). Contextual approaches to cybersecurity research in Nigeria. African Journal of ICT Policy and Governance, 15(1), 34–48.

Markopoulou, D., & Papakonstantinou, V. (2021). Metrics for cybersecurity policy effectiveness in critical infrastructure protection. Journal of Cyber Policy, 6(2), 123–145.

Nguyen, L. H., Tan, W. L., & Rahman, S. (2023). Cybersecurity governance in Southeast Asia: Comparative insights from Vietnam and Malaysia. Asian Journal of Policy Studies, 12(2), 84–103.

NIST. (2024, February 26). NIST releases version 2.0 of landmark cybersecurity framework (Press release). https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework.

NIST. (2024). NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Okoye, N. S., Uchenna, T. U., & Okechukwu, I. E. (2023). Addressing digital technology gap challenges: The Nigerian experience. NG Journal of Social Development, 11(1), 95-100.

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. Administration and Policy in Mental Health and Mental Health Services Research, 42(5), 533–544. https://doi.org/10.1007/s10488-013-0528-y.

Pollini, A., Seigel, A., Baecker, R. M., & Faily, S. (2021). Leveraging human factors in cybersecurity: An integrated approach and research agenda. Frontiers in Psychology, 12, Article 673794. https://doi.org/10.3389/fpsyg.2021.673794.

Sibe, R., & Kaunert, C. (2024). Cybersecurity governance challenges in resource-constrained nations. Journal of Global Security Studies, 9(1), 22–39.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487–502.

World Economic Forum. (2023). Global Cybersecurity Outlook 2023. Geneva: World Economic Forum. Retrieved from https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf.

Zenarmor. (2023). The NIST Cybersecurity Framework explained. Zenarmor Research Reports. Retrieved from https://www.zenarmor.com/docs/network-security-tutorials/what-is-nist-cybersecurity-framework.

Sabatier, P., & Mazmanian, D. (1979). the implementation of public policy: a framework of analysis. *Policy Studies Journal*, 8(4), 538-560. https://doi.org/10.1111/j.1541-0072.1980.tb01266.x.

Ogene, F. (2024). Cybersecurity and IT Governance Challenges in Nigeria: Strategic Investment Needs and the Path Forward for a Resilient Digital Economy. International Journal of Computer Applications, 186(55).

Ojuri, M. A. (2022). *Cybersecurity maturity models as a quality assurance tool for African organisations* (Article). https://smsjournals.com/index.php/SAMRIDDHI/article/download/3416/1737.

ISO. (2022). ISO/IEC 27001:2022 — Information security management systems — Requirements. https://www.iso.org/standard/27001.

Badamasi, B., & Utulu, S. C. A. (2021). Framework for Managing Cybercrime Risks in Nigerian Universities. arXiv. https://arxiv.org/abs/2108.09754.

Jonah, K. (2023). A Comparative Analysis of the Nigerian Data Protection Act 2023 and the EU General Data Protection Regulations Applicable in the United Kingdom. SSRN.

Yamane, T. (1967). Statistics: An introductory analysis (2nd ed.). Harper & Row, 886.

Zhang, X., Li, J., & Chen, Y. (2024). Resistance to change in cybersecurity policy adoption. Computers & Security, 133, 103190.