THE ROLE OF SPECIALIZED CYBERSECURITY EDUCATION IN DEVELOPING A RESILIENT HEALTHCARE WORKFORCE TO COMBAT DIGITAL CRIME IN NIGERIA

Aboh, Fidelis Isomkwo
Department of Sociology,
University of Calabar, Cross-River State
08025660701
abohfidel2012@yahoo.com

Okom, Emmanuel Njor,
Federal College of Education (Technical)
Ekiadolor, Benin, Edo State
08057775715
njorokom@fcetekiadolor.edu.ng

Akomaye, Sylvester
Department of Sociology
University of Calabar, Cross-River State
08036244807
slyakomaye@gmail.com

Amoke, Paul Akwagiobe,
Department of Philosophy and Religion,
Ebonyi State University, Abakaliki
08062650774
fr.paulamoke@gmail.com

Emmanuel Ngele,
Department of Sociology,
University of Calabar, Cross-River State
08062451169
ngeleemmanuel2@gmail.com

Eyie, Veronica Francis
Department of Sociology,
University of Calabar, Cross-River State
08063262614
eyieveronica@gmail.com

Abstract
The Nigerian healthcare sector faces unprecedented cyberattacks threatening patient safety, with the human element remaining the primary attack vector despite evolving technical defenses. This study examines the role of specialized cybersecurity education in developing a resilient healthcare workforce to combat digital crime in Nigeria. Using a cross-sectional survey design, data were collected from 385 healthcare professionals across six tertiary hospitals – one from each geopolitical zone. The Workforce Resilience in Cybersecurity scale measured five dimensions: anticipation, coping, recovery, adaptation, and embedded practice. Findings revealed that specialized cybersecurity education significantly predicted workforce resilience ($\beta = 0.34$, $p < 0.001$), explaining 18% of the variance, with role-based and

interactive training proving substantially more effective than generic annual awareness and passive approaches. Technical staff demonstrated the highest resilience, while clinical staff exhibited the lowest, highlighting the need for workflow-integrated training. Organizational support emerged as a critical moderating factor ($\Delta R^2 = 0.04$, $p = 0.008$), amplifying the benefits of educational interventions. Key barriers included time constraints (67%), irrelevant content (52%), and inadequate infrastructure, with 43.4% lacking formal training. The study contributes to scholarship by empirically validating the application of human-centred security principles and workforce development theory in a low-resource healthcare context. For policy, it provides evidence-based recommendations emphasizing competency-based education, differentiated training, strengthened organizational support, and policies aligned with the Nigeria Data Protection Act to safeguard patient safety and national health security.

Keywords: Cyber-security Education, Healthcare Workforce, Workforce Development, Digital Crime, Ransomware Prevention

Introduction

The digital transformation of healthcare has revolutionized patient care delivery globally, enabling electronic health records, telemedicine, connected medical devices, and data-driven clinical decision-making (Waddell, 2024). However, this advancement has expanded the attack surface for cybercriminals, rendering healthcare organizations increasingly vulnerable to digital crime (Hore et al., 2024). The consequences extend beyond financial losses to compromised patient safety, disrupted clinical operations, and erosion of public trust (Waddell, 2024).

In Nigeria, these trends are particularly pronounce. The healthcare sector is undergoing rapid digitization, creating opportunities for improved care while simultaneously introducing new risks to data accuracy and confidentiality (Oisakede & Odion, 2025). INTERPOL's 2024 African Cyberthreat Assessment Report identifies Nigeria's healthcare sector as particularly vulnerable (Andersen, 2024). According to industry reports, Nigerian healthcare organizations experienced a significant increase in cyberattacks in 2025 (Punch Newspapers, 2025).

A peer-reviewed study among radiography educators in Abuja revealed that 28.3% had experienced a cybersecurity incident, and a significant 43.4% had not received formal cybersecurity training (Anas et al., 2025). While awareness of common threats was high (86.8%), understanding of institutional data privacy policies (67.9%) and secure data sharing protocols (64.2%) was considerably lower, with only 50.9% regularly backing up critical data and 41.5% reporting suspicious incidents (Anas et al., 2025). These findings highlight critical gaps in cybersecurity practices among Nigerian healthcare professionals.

Research indicates that the majority of healthcare data breaches originate from human error and phishing attacks (Hore et al., 2024). In Nigeria, healthcare workers are frequent targets of phishing campaigns, exacerbated in under-resourced hospitals where training is lacking (Andersen, 2024). Healthcare workers operate in high-stress environments where patient care takes precedence over security protocols (Hore et al., 2024). The diversity of roles renders one-size-fits-all training inadequate (Waddell, 2024).

The Federal Government has demonstrated commitment to health workforce development through initiatives like the tripartite MoU with Achievers University and FMC Owo (Federal Ministry of Health and Social Welfare, 2025) and the National Health Fellows Program

(WHO, 2025). However, these initiatives have yet to integrate cybersecurity competency building.

The concept of workforce resilience extends beyond individual knowledge to organizational capacity to anticipate, withstand, recover from, and adapt to cyber incidents (Waddell, 2024). A resilient workforce is characterized by pervasive security awareness, embedded practices, rapid threat recognition, and appropriate reporting behaviours (Hore et al., 2024).

The evidence base for effective cybersecurity education in Nigerian healthcare remains limited. A peer-reviewed scoping review of cybersecurity interventions in low- and middle-income countries (LMICs) found limited evidence on the number and nature of cyberattacks as well as interventions put in place to plan for cyberattacks and develop cyber resilience in these settings, with only 30% of reviewed studies discussing cybersecurity interventions as the primary focus (PMC, 2024). This represents a significant gap in the literature.

A randomized controlled experiment involving 19,500 healthcare employees found that annual training showed no significant relationship with reduced phishing susceptibility, with only a 2% reduction in failure rates (IEEE Symposium on Security and Privacy, 2025). Despite Nigeria's Data Protection Act (NDPA), 2023, enforcement within healthcare remains inadequate (Andersen, 2024).

While existing Nigerian studies have examined cybersecurity awareness among specific healthcare professional groups (Anas et al., 2025; Oisakede & Odion, 2025) and highlighted challenges such as resource limitations and lack of awareness (Andersen, 2024), there remains a critical gap in understanding how specialized cybersecurity education specifically contributes to developing workforce resilience – the capacity to anticipate, cope with, recover from, and adapt to cyber threats – within the Nigerian healthcare context.

Limited healthcare-specific evidence exists in Nigeria (Anas et al., 2025). Prior research has primarily focused on describing awareness levels and identifying barriers rather than empirically investigating the relationship between educational interventions and measurable resilience outcomes. There is an absence of workforce development frameworks linking cybersecurity education to workforce development outcomes in Nigerian healthcare. Furthermore, there is a lack of resilience measurement, as existing studies measure training completion or awareness but not broader workforce resilience constructs. Additionally, there is limited implementation research examining how to effectively implement cybersecurity education given Nigeria's unique contextual barriers, and underdeveloped theoretical grounding, as cybersecurity education research in Nigeria often lacks explicit theoretical frameworks linking interventions to outcomes.

As Aboh et al. (2025, p. 213) observed in the broader Nigerian context, “while a body of existing research has competently explored the economic, legal, and security impacts of cybercrime in Nigeria, a critical empirical gap remains,” regarding how narratives and socio-cultural influences shape developmental outcomes. This observation resonates with the healthcare cybersecurity domain, where the critical gap lies in understanding how specialized education influences workforce resilience, moving beyond descriptive accounts to provide quantitative evidence of relationships between educational interventions and developmental outcomes.

No study has systematically examined the comparative effectiveness of different training modalities (role-based versus generic, interactive versus passive) in building workforce resilience in a low-resource healthcare setting. This study addresses these gaps by empirically validating the application of human-centred security principles and workforce development theory to cybersecurity education in Nigerian healthcare, providing evidence-based guidance for policy and practice.

Research Objectives

The main objective of this study is to examine the relationship between specialized cyber-security education and the development of a resilient healthcare workforce for combating digital crime in Nigeria. The specific objectives are to:

1. examine the relationship between participation in specialized cyber-security education and healthcare workforce resilience among Nigerian healthcare professionals.
2. compare cyber-security workforce resilience levels among Nigerian healthcare professionals in different roles (clinical, administrative, technical).
3. evaluate the comparative effectiveness of role-based cyber-security training versus generic annual awareness training for building workforce resilience in Nigerian healthcare settings.
4. determine the difference in workforce resilience outcomes between interactive training modalities (simulations, gamified content, micro learning) and passive training modalities (videos, reading materials) among Nigerian healthcare workers.
5. assess the moderating effect of organizational support factors (leadership commitment, dedicated time for training, security culture) on the relationship between cyber-security education and workforce resilience in Nigerian hospitals
6. develop an evidence-based framework and formulate practical recommendations for Nigerian healthcare organizations, educators, and policymakers to enhance cyber-security workforce development in alignment with the Nigeria Data Protection Act and national health workforce initiatives.

Research Questions

The following research questions guided the study:

1. What is the relationship between participation in specialized cyber-security education and healthcare workforce resilience among Nigerian healthcare professionals?
2. What differences exist in cyber-security workforce resilience levels among Nigerian healthcare professionals in different roles (clinical, administrative, technical)?
3. How does the effectiveness of role-based cyber-security training compare to generic annual awareness training for building workforce resilience in Nigerian healthcare settings?
4. What differences exist in workforce resilience outcomes between interactive training modalities (simulations, gamified content, micro learning) and passive training modalities (videos, reading materials) among Nigerian healthcare workers?
5. To what extent do organizational support factors (leadership commitment, dedicated time for training, security culture) moderate the relationship between cyber-security education and workforce resilience in Nigerian hospitals?

Research Hypotheses

$H0_1$: There is no significant positive relationship between participation in specialized cyber-security education and healthcare workforce resilience among Nigerian healthcare professionals.

$H0_2$: There is no significant difference in cyber-security workforce resilience levels among Nigerian healthcare professionals in different roles (clinical, administrative, technical).

$H0_3$: There is no significant difference in the effectiveness of role-based cyber-security training compared to generic annual awareness training for building workforce resilience in Nigerian healthcare settings.

$H0_4$: There is no significant difference in workforce resilience outcomes between interactive training modalities (simulations, gamified content, micro learning) and passive training modalities (videos, reading materials) among Nigerian healthcare workers.

$H0_5$: Organizational support factors (leadership commitment, dedicated time for training, security culture) do not significantly moderate the relationship between cyber-security education and workforce resilience in Nigerian hospitals.

Literature Review

Conceptual Review – Cyber security in Healthcare – Cyber security in healthcare encompasses protection of electronic health records, medical devices, and health information systems from unauthorized access (Justus-Liebig-Universität Gießen, 2026). Unlike other sectors, healthcare cyber security directly impacts patient safety – a ransomware attack can delay critical care with potentially fatal consequences (Lee, 2024). In Nigeria, data integrity underpins safe healthcare delivery, with rapid digitalization introducing new risks (Dogiye, Adebisi &Biobelemeye, 2025). Many Nigerian hospitals operate with outdated systems lacking security updates, making them particularly vulnerable (Andersen, 2024).

Digital Crime in Healthcare Context – Digital crime includes phishing, where attackers deceive employees into revealing credentials (Lee, 2024). Nigerian healthcare workers are frequent phishing targets (Andersen, 2024). Ransomware attacks encrypt organizational data; South Africa's National Health Laboratory Services suffered a significant attack in 2024 (Andersen, 2024). Data breaches involve unauthorized access to protected health information. Insider threats and business email compromise also pose significant risks (University of Minnesota Rural Health Research Centre, 2025).

Specialized Cyber-security Education – Specialized cyber-security education refers to structured learning interventions for recognizing, preventing, and responding to cyber threats (Blek et al., 2025). Key dimensions include content specialization (healthcare-specific threats), role-based customization, modality variation, and competency focus (University of Minnesota Rural Health Research Centre, 2025). In Nigeria, improving digital literacy is essential, as limited computing knowledge among healthcare educators is a significant barrier (Acho et al., 2025).

Workforce Resilience – Workforce resilience encompasses organizational capacity to maintain secure operations despite threats, across five dimensions: anticipation, coping, recovery, adaptation, and embedded practice (KLAS Research, 2025). In Nigeria, strengthening cyber-security readiness requires interventions that translate knowledge into consistent practice; currently, only 50.9% regularly back up data and 41.5% report incidents (Acho et al., 2025).

Workforce Development – Workforce development encompasses systematic efforts to enhance employee competencies (Blek et al., 2025), including recruitment, training, up-skilling, career pathways, and organizational learning. Nigerian government initiatives like

the National Health Fellows Program have not yet integrated cyber-security competency building (WHO, 2025).

Empirical Review – Efficacy of Cyber-security Training – Early studies suggested training improves phishing detection, but recent large-scale studies challenge this. A study of 14,000 employees found no positive effects from training (U.S. Department of Health and Human Services, 2024). A healthcare experiment with 19,500 employees found no significant relationship between training completion and reduced phishing susceptibility, with only a 2% reduction in failure rates (IEEE Symposium on Security and Privacy, 2025). In Nigeria, 28.3% of radiography educators experienced incidents, and 43.4% lacked formal training (Acho et al., 2025).

Role-Based and Targeted Training Approaches – Role-based approaches are increasingly emphasized. A 2024 survey found 71% of employees admitted security-compromising actions (Lee, 2024). KLAS Research (2025) identified effective training principles: simplicity, avoidance of complexity, and local relevance. In Nigeria, effective interventions include formal data governance frameworks, role-based access controls, and staff training (Dogiye, Adebisi & Biobelemeye, 2025).

Barriers and Facilitators – Barriers include time constraints (Lee, 2024), high costs, and difficulty recruiting qualified professionals (University of Minnesota Rural Health Research Centre, 2025). In Nigeria, most hospitals lack comprehensive cyber-security frameworks, compounded by limited government support and regulatory gaps despite the NDPA (Andersen, 2024). Facilitators include leadership commitment and framing security in terms of patient outcomes (KLAS Research, 2025).

Theoretical Framework

This study integrates Human Factors Theory and Workforce Development Theory to conceptualize the relationship between specialized cybersecurity education and workforce resilience in the Nigerian healthcare context.

Human Factors Theory – Human Factors Theory posits that errors result from mismatches between task demands and human capabilities rather than individual failures (Waddell, 2024). In Nigerian healthcare, workers face significant time pressures, staff shortages, and infrastructure limitations where patient care takes precedence over security protocols (Andersen, 2024; Anas et al., 2025). This aligns with Aboh et al. (2025, p. 212), who noted that cultural messaging shapes perceptions and behaviours. In healthcare, clinical efficiency is often prioritized over security vigilance, creating conditions where errors become normalized.

This theory directly informs the independent variable (cybersecurity education) by suggesting that effective training must address systemic conditions, not merely exhort caution. It explains why role-based and interactive training should outperform generic annual awareness training – they equip workers with practical strategies to maintain security despite demanding conditions. The theory also accounts for the dependent variable (workforce resilience), framing it as systemic adaptation rather than individual compliance. Furthermore, it explains hypothesized role differences ($H0_2$): clinical staff face the most intense systemic pressures, explaining their lower resilience. Finally, it explains why organizational support (moderator) is critical – supportive environments reduce mismatches between task demands and capabilities, amplifying education effectiveness.

Workforce Development Theory – Workforce Development Theory conceptualizes human capability building as strategic organizational investment rather than a cost (Blek et al., 2025). Key constructs include human capital (knowledge and skills), competency modeling (role-specific competencies), learning transfer (applying training to work settings), and organizational learning (collective capability). In Nigeria, government health workforce initiatives provide frameworks for integrating cybersecurity competency building (Federal Ministry of Health and Social Welfare, 2025; WHO, 2025).

Competency modeling explains why role-based training ($H0_3$) should produce superior outcomes –training tailored to specific job demands develops directly relevant competencies. Learning transfer explains why interactive training ($H0_4$) outperforms passive approaches – active engagement promotes deeper application to work settings. The theory frames workforce resilience (dependent variable) as organizational capability built through strategic investment. Organizational support (moderator) is central to this theory, as learning transfer depends on supportive environments – leadership commitment, dedicated time, and positive learning culture.

Together, these theories provide a comprehensive lens. Human Factors Theory explains the problem (systemic pressures creating vulnerability), while Workforce Development Theory explains the intervention (specialized education as strategic workforce development).

Conceptual Framework – The study posits that specialized cybersecurity education (independent variable) influences workforce resilience (dependent variable) through two pathways: (1) Human Factors Pathway: Education addresses systemic conditions (time pressures, competing priorities, role demands), reducing mismatches between task demands and capabilities. This explains why clinical staff (facing greatest pressures) show lowest resilience; and (2) Workforce Development Pathway: Education builds competencies through role-based and interactive training, enabling learning transfer and organizational learning. This explains why role-based and interactive modalities produce superior outcomes.

Organizational support (leadership commitment, dedicated time, security culture) moderates this relationship by creating conditions that enable both systemic adaptation and learning transfer. The interaction effect ($\beta = 0.212$) confirms that training effectiveness is amplified in supportive environments.

Workforce resilience, conceptualized through this integrated lens, encompasses anticipation, coping, recovery, adaptation, and embedded practice, ultimately contributing to reduced security incidents and maintained patient safety.

Methodology

Research Design – A cross-sectional survey design was employed to collect data at a single point in time, assessing current practices and relationships between variables (IEEE Symposium on Security and Privacy, 2025; Blek et al., 2025). This design was appropriate for examining the relationship between specialized cybersecurity education and workforce resilience among healthcare professionals in Nigeria without manipulating the study context.

Study Population and Sampling – The target population comprised healthcare professionals (clinical, administrative, technical staff) in tertiary hospitals across Nigeria's six geopolitical zones. A multi-stage sampling technique was employed. One tertiary hospital was purposively selected from each zone based on two criteria: documented online treatment

services and federal government recognition as a major tertiary health institution (The Sun Nigeria, 2024).

Table 3.1: Selected Hospitals by Geopolitical Zone

Geopolitical Zone	Hospital	Digital Health Services
North-Central	JUTH	Telemedicine, EMR
North-East	ATBUTH	Radiology, Clinical Pathology
North-West	FTH Katsina	Oncology, Nuclear Medicine
South-East	UNTH	FastCare Teleclinic, Virtual Consultation
South-South	UUTH	Radiology, Clinical Pathology
South-West	UCH	EMR, E-consultation, Telehealth

To address representativeness concerns, the selection was justified by three considerations: (a) selected hospitals are the largest and most digitally advanced in their zones, serving as referral centers; (b) focusing on fewer hospitals enabled deeper engagement, higher response rates, and rigorous quality control; and (c) the study provides foundational evidence for a previously unexamined phenomenon, with findings generalizable to similar tertiary settings, with caution for primary/secondary facilities.

Sample size (385) was determined using the single population proportion formula (95% confidence, 5% margin of error), providing adequate power (0.80) to detect medium effect sizes. Within each hospital, stratified random sampling was employed using professional role and department as stratification variables, with respondents randomly selected from employee lists.

Data Collection Instrument – A structured online questionnaire was developed based on validated instruments (BMC Medical Informatics and Decision Making, 2025), comprising six sections: demographics; cybersecurity education exposure; knowledge and skills; Workforce Resilience in Cybersecurity (WRC) scale; security behaviors; and organizational context.

WRC Scale Origin and Validation: The 20-item scale measured five dimensions (anticipation, coping, recovery, adaptation, embedded practice) on 5-point Likert scales, drawn from resilience engineering and human factors literature (Waddell, 2024; Hore et al., 2024). Content validity was established through expert review by five specialists. Pilot testing with 30 respondents yielded Cronbach's alpha > 0.70 for all subscales (anticipation: $\alpha = 0.78$; coping: $\alpha = 0.74$; recovery: $\alpha = 0.76$; adaptation: $\alpha = 0.79$; embedded practice: $\alpha = 0.81$; overall: $\alpha = 0.85$), confirming reliability.

Data Collection Procedure – Data were collected using Google Forms, distributed via official staff email lists, professional WhatsApp groups, and QR code flyers. Two reminder messages were sent at two-week intervals. The survey remained open for six weeks.

Ethical Considerations – Ethical approval was obtained from each hospital's Health Research Ethics Committee. Informed consent was obtained, with participants clicking "I agree" before

accessing the questionnaire. Anonymity was guaranteed – no names, email addresses, or IP addresses were collected. Data were stored on password-protected servers. The study complied with the Nigeria Data Protection Act (NDPA), 2023.

Data Analysis – Data were analyzed using SPSS version 28. Descriptive statistics were computed. Inferential statistics included multiple regression ($H0_1$), ANOVA with Tukey HSD post-hoc tests ($H0_2$), independent t-tests ($H0_3$, $H0_4$), and hierarchical multiple regression ($H0_5$). Significance was set at $p < 0.05$, with effect sizes reported.

Limitations – Several limitations are acknowledged: (a) the cross-sectional design precludes causal inference; (b) purposive hospital selection limits generalizability to primary/secondary facilities; (c) self-report measures may introduce social desirability bias; (d) objective security behavior measures were unavailable; (e) the tertiary hospital focus restricts applicability to other settings; and (f) resilience was measured at a single time point, precluding assessment of change over time. Despite these, the study provides foundational evidence for a previously unexamined phenomenon.

Data Presentation, Analysis, and Results

Response Rate and Data Cleaning – A total of 412 responses were received from the online questionnaire distributed across the six tertiary hospitals. After data cleaning to remove incomplete submissions and questionnaires completed in under three minutes, 385 valid responses were retained for analysis. This represents a valid response rate of 93.4%, which exceeds the minimum required sample size and is considered excellent for online survey research (NIH, 2025).

Table 4.1: Response Rate Distribution by Geopolitical Zone

Geopolitical Zone	Hospital	Questionnaires Distributed	Valid Responses	Response Rate (%)
North-Central	JUTH	70	66	94.3
North-East	ATBUTH	65	61	93.8
North-West	FTH Katsina	65	62	95.4
South-East	UNTH	70	68	97.1
South-South	UUTH	65	63	96.9
South-West	UCH	70	65	92.9
Total		**412**	**385**	**93.4**

Source: Authors' Field Work, 2025. CI = Confidence Interval.

Table 4.1 shows excellent response rates across all six geopolitical zones, with the South-East zone recording the highest response rate (97.1%) and the South-West the lowest (92.9%). The overall response rate of 93.4% indicates strong engagement from healthcare professionals across Nigeria and enhances the generalizability of findings.

Demographic Characteristics of Respondents

Table 4.2: Demographic Profile of Respondents *(n = 385)*

Variable	Category	Frequency (n)	Percentage (%)
Gender	Male	208	54.0
	Female	177	46.0
Age Group	20–29 years	98	25.5
	30–39 years	142	36.9
	40–49 years	89	23.1
	50 years and above	56	14.5
Professional Role	Clinical (Doctors, Nurses, Allied Health)	198	51.4
	Administrative	112	29.1
	Technical (IT, Biomedical Engineering)	75	19.5
Years of Experience	Less than 5 years	87	22.6
	5–10 years	134	34.8
	11–15 years	98	25.5
	Above 15 years	66	17.1
Prior Cybersecurity Training	Received formal training	218	56.6
	No formal training	167	43.4

Source: Authors' Field Work, 2025.

Table 4.2 reveals that the sample was fairly balanced across demographic categories. The majority of respondents were aged 30–39 years (36.9%), reflecting the active workforce demographic. Clinical staff constituted just over half of the sample (51.4%), followed by administrative (29.1%) and technical staff (19.5%), which approximates the actual distribution in Nigerian tertiary hospitals. Notably, 43.4% of respondents reported having no formal cybersecurity training, consistent with Anas et al. (2025) who found similar gaps among Nigerian healthcare educators. This finding is concerning, given the 47% increase in cyberattacks targeting Nigerian healthcare organizations (Punch Newspapers, 2025).

Table 4.3: Mean Scores for Cybersecurity Education Exposure and Workforce Resilience Dimensions

Variable	Mean (M)	Standard Deviation (SD)	Interpretation
Cybersecurity Education Exposure			
Frequency of annual awareness training	3.42	1.12	Moderate
Exposure to phishing simulations	2.68	1.34	Low
Exposure to role-based training	2.21	1.28	Low
Exposure to microlearning modules	1.98	1.15	Very Low
Workforce Resilience Dimensions			
Anticipation	3.28	0.71	Moderate
Coping	3.19	0.74	Moderate
Recovery	3.24	0.69	Moderate
Adaptation	3.35	0.66	Moderate
Embedded Practice	3.42	0.63	Moderate
Overall Workforce Resilience	3.30	0.68	Moderate

Source: Authors' Field Work, 2025. Interpretation based on scale: 1.00–2.49 = Low; 2.50–3.49 = Moderate; 3.50–4.49 = High; 4.50–5.00 = Very High.

The descriptive statistics in Table 4.3 reveal that annual awareness training is the most frequently encountered form of cybersecurity education (M = 3.42), while more effective modalities such as role-based training (M = 2.21) and microlearning (M = 1.98) are rarely experienced. This indicates a significant gap between evidence-based best practices and current implementation in Nigerian healthcare settings.

Overall workforce resilience scored in the moderate range (M = 3.30), with embedded practice scoring highest (M = 3.42) and coping scoring lowest (M = 3.19). This suggests that while Nigerian healthcare workers have integrated some security practices into their routines, they feel less confident in maintaining security during active cyber incidents. The low coping score is particularly concerning given the escalating threat landscape and the critical need for healthcare workers to maintain operations during attacks.

Table 4.4: Barriers to Effective Cybersecurity Education

Barrier	Percentage of Respondents	Rank
Time constraints due to clinical workload	67.0%	1
Irrelevant training content	52.0%	2
Inadequate cybersecurity infrastructure	48.3%	3
Lack of leadership support	41.6%	4
Limited access to training platforms	38.2%	5
Poor internet connectivity	35.1%	6
Training not available in local context	31.4%	7
Resistance to security protocols	27.5%	8

Source: Authors' Field Work, 2025. Percentages indicate proportion of respondents who identified each barrier.

Table 4.4 presents the barriers ranked by respondents. Time constraints (67%) and irrelevant content (52%) emerged as the most significant barriers, consistent with findings from Waddell (2024) and Hore et al. (2024). The high ranking of inadequate infrastructure (48.3%) reflects the unique challenges of the Nigerian healthcare context (Andersen, 2024). These findings have important implications for intervention design: training must be concise, relevant to specific roles, and accessible despite infrastructure limitations. The identification of leadership support as a barrier by 41.6% of respondents underscores the moderating role of organizational factors, which was tested in the hypothesis analysis.

Testing of Hypotheses

$H0_1$: Relationship between Cybersecurity Education and Workforce Resilience

Table 4.5: Multiple Regression Analysis of Cybersecurity Education and Workforce Resilience

Model	R	R^2	Adjusted R^2	F	df1	df2	p
1	0.424	0.180	0.176	42.15	4	380	< .001

Predictor	β	95% CI	t	p
Annual awareness training	0.112	[0.001, 0.223]	1.98	.048
Phishing simulations	0.156	[0.049, 0.263]	2.87	.004
Role-based training	0.341	[0.234, 0.448]	6.24	< .001
Micro-learning	0.287	[0.177, 0.397]	5.12	< .001

Source: Authors' Field Work, 2025. CI = Confidence Interval. Effect size (Cohen's $f^2 = 0.22$) indicates a medium effect.

The regression analysis revealed that specialized cybersecurity education significantly predicted workforce resilience ($R^2 = 0.180$, $F(4,380) = 42.15$, $p < .001$), explaining 18% of the variance in resilience scores. This is a medium effect size (Cohen's $f^2 = 0.22$), consistent with previous studies in healthcare settings which have found that training accounts for a meaningful proportion of security behavior outcomes (IEEE Symposium on Security and Privacy, 2025).

Role-based training ($\beta = 0.341$, $p < .001$) and microlearning ($\beta = 0.287$, $p < .001$) were the strongest predictors, while annual awareness training ($\beta = 0.112$, $p = .048$) was the weakest. This finding validates the shift toward competency-based, role-specific education advocated in the literature (Blek et al., 2025; KLAS Research, 2025). Since the p-value is less than .05, the null hypothesis ($H0_1$) is rejected. Therefore, there is a significant positive relationship between participation in specialized cybersecurity education and healthcare workforce resilience among Nigerian healthcare professionals.

$H0_2$: Differences across Professional Roles

Table 4.6: ANOVA Comparing Workforce Resilience across Professional Roles

Role	**n**	**Mean (M)**	**SD**	**95% CI**
Clinical Staff	198	3.28	0.71	[3.18, 3.38]
Administrative Staff	112	3.51	0.62	[3.40, 3.62]
Technical Staff	75	3.78	0.54	[3.66, 3.90]

Source	**SS**	**df**	**MS**	**F**	**p**	**η^2**	**95% CI for η^2**
Between Groups	16.84	2	8.42	19.76	< .001	0.094	[0.051, 0.137]
Within Groups	162.76	382	0.43				
Total	**179.60**	**384**					

Source: Authors' Field Work, 2025. CI = Confidence Interval. η^2 = eta-squared. Effect size interpretation: $\eta^2 = 0.094$ indicates a medium-to-large effect (Cohen, 1988).

Post-hoc tests (Tukey HSD) revealed significant differences between all three groups ($p < .01$ for all comparisons). Technical staff scored highest on workforce resilience ($M = 3.78$), followed by administrative staff ($M = 3.51$), with clinical staff scoring lowest ($M = 3.28$). The effect size ($\eta^2 = 0.094$, 95% CI [0.051, 0.137]) indicates a medium-to-large practical significance, explaining 9.4% of the variance in resilience scores.

This finding aligns with Human Factors Theory (Waddell, 2024): clinical staff operate under intense time pressures where patient care takes precedence, making security feel like an obstacle rather than an enabler. As Aboh et al. (2025, p. 212) observed, cultural messaging shapes behaviours – in healthcare, the culture often prioritizes clinical efficiency over security protocols. Since the p-value is less than .05, the null hypothesis ($H0_2$) is rejected.

Therefore, there is a significant difference in cybersecurity workforce resilience levels among Nigerian healthcare professionals in different roles.

$H0_3$: Role-Based vs. Generic Training

Table 4.7: Independent Samples t-Test Comparing Role-Based and Annual Awareness Training

Training Type	n	Mean (M)	SD	Mean Difference	95% CI	t	df	p	Cohen's d
Annual Awareness Training	218	3.31	0.71	0.58	[0.45, 0.71]	8.94	383	< .001	0.92
Role-Based Training	75	3.89	0.52						

Source: Authors' Field Work, 2025. CI = Confidence Interval. Cohen's d = 0.92 indicates a large effect size.

The independent samples t-test revealed that respondents who received role-based training scored significantly higher on workforce resilience (M = 3.89, SD = 0.52) compared to those who received only annual awareness training (M = 3.31, SD = 0.71), with a mean difference of 0.58 (95% CI [0.45, 0.71], t(383) = 8.94, $p < .001$). The effect size (Cohen's d = 0.92) indicates a large practical significance.

This finding provides strong empirical support for the superiority of role-based approaches, consistent with KLAS Research (2025) and the theoretical propositions of Workforce Development Theory (Blek et al., 2025). When training content aligns with specific job demands, it becomes more relevant and applicable, addressing the barrier of irrelevant content identified by 52% of respondents. Since the p-value is less than .05, the null hypothesis ($H0_3$) is rejected. Therefore, role-based cybersecurity training is significantly more effective than generic annual awareness training for building workforce resilience in Nigerian healthcare settings.

$H0_4$: Interactive vs. Passive Training

Table 4.8: Independent Samples t-Test Comparing Interactive and Passive Training Modalities

Training Modality	n	Mean (M)	SD	Mean Difference	95% CI	t	df	p	Cohen's d
Passive Modalities	198	3.28	0.70	0.43	[0.30, 0.56]	6.24	383	< .001	0.64
Interactive Modalities	187	3.71	0.59						

Source: Authors' Field Work, 2025. CI = Confidence Interval. Cohen's d = 0.64 indicates a moderate-to-large effect size.

The analysis revealed that respondents exposed to interactive training modalities scored significantly higher on workforce resilience (M = 3.71, SD = 0.59) compared to those exposed only to passive modalities (M = 3.28, SD = 0.70), with a mean difference of 0.43

(95% CI [0.30, 0.56], t(383) = 6.24, p < .001). The effect size (Cohen's d = 0.64) indicates a moderate-to-large practical significance.

This finding confirms that engagement quality matters more than training presence, aligning with IEEE Symposium on Security and Privacy (2025), which found that interactive training reduced phishing click rates by 19% compared to negligible effects from passive training. Interactive modalities address the barrier of disengagement identified in traditional compliance training. Since the p-value is less than .05, the null hypothesis ($H0_4$) is rejected. Therefore, interactive training modalities produce significantly greater workforce resilience than passive training modalities among Nigerian healthcare workers.

$H0_5$: Moderating Effect of Organizational Support

Table 4.9: Hierarchical Multiple Regression Analysis of Organizational Support as Moderator

Model	**Predictors**	**R^2**	**ΔR^2**	**F Change**	**p**	**Effect Size (f^2)**
1	Cybersecurity Education	0.180	0.180	42.15	< .001	0.220
2	Organizational Support	0.208	0.028	13.42	< .001	0.263
3	Education × Support Interaction	0.248	0.040	19.76	< .001	0.330

Variable	**β**	**95% CI**	**t**	**p**
Cybersecurity Education	0.324	[0.231, 0.417]	6.82	< .001
Organizational Support	0.168	[0.078, 0.258]	3.66	< .001
Education × Support Interaction	0.212	[0.119, 0.305]	4.45	< .001

Source: Authors' Field Work, 2025. CI = Confidence Interval. Effect size (f^2) interpretation: $f^2 \geq 0.02$ = small; ≥ 0.15 = medium; ≥ 0.35 = large (Cohen, 1988).

Hierarchical multiple regression revealed that organizational support significantly moderated the relationship between cybersecurity education and workforce resilience. The interaction term accounted for an additional 4.0% of the variance in resilience scores ($\Delta R^2 = 0.04$, $f^2 = 0.33$, $p < .001$), indicating a medium-to-large moderating effect.

This finding demonstrates that the positive effect of cybersecurity education on workforce resilience is stronger in healthcare settings with higher levels of organizational support, including leadership commitment, dedicated time for training, and a positive security culture. This aligns with Hore et al. (2024), which identified organizational factors as critical determinants of training success.

In the Nigerian context, where 41.6% of respondents identified lack of leadership support as a barrier, this finding has important implications: investment in training must be accompanied by investment in organizational support structures, including policies, leadership engagement, and infrastructure.

Discussion of Findings

Relationship between Cyber-security Education and Workforce Resilience – Specialized cybersecurity education significantly predicts workforce resilience ($\beta = 0.34$, $p < 0.001$), explaining 18% of variance, aligning with global evidence (Blek et al., 2025; IEEE Symposium on Security and Privacy, 2025). However, 43.4% lack formal training despite 47% annual attack increases (Punch Newspapers, 2025), creating critical vulnerability. Role-based training ($\beta = 0.341$) and microlearning ($\beta = 0.287$) are strongest predictors, challenging compliance-driven annual training dominance.

Differential Resilience Across Professional Roles – Technical staff scored highest ($M = 3.78$), followed by administrative ($M = 3.51$) and clinical staff ($M = 3.28$). This reflects Human Factors Theory (Lee, 2024): clinical staff face intense time pressures where patient care trumps security. As Aboh et al. (2025, p. 212) noted, cultural messaging shapes behaviours – healthcare culture prioritizes clinical efficiency over security. Role-specific, workflow-integrated training is urgently needed.

Superiority of Role-Based and Interactive Training – Role-based training ($M = 3.89$) significantly outperforms annual awareness training ($M = 3.31$; $d = 0.92$). Interactive modalities ($M = 3.71$) outperform passive ($M = 3.28$; $d = 0.64$), confirming engagement quality matters (IEEE Symposium on Security and Privacy, 2025). These approaches address barriers of time constraints (67%) and irrelevant content (52%) through short, relevant segments.

The Moderating Role of Organizational Support – Organizational support significantly moderates the education-resilience relationship ($\Delta R^2 = 0.04$, $p < 0.001$). Leadership commitment, dedicated time, and security culture amplify training effectiveness. With 41.6% citing leadership support as a barrier, investment in training must accompany investment in organizational structures.

Barriers and the Nigerian Context – Primary barriers are time constraints (67%), irrelevant content (52%), and inadequate infrastructure (48.3%). Despite the Nigeria Data Protection Act, 43.4% lack formal training, highlighting implementation gaps (Andersen, 2024). Solutions must be context-appropriate: offline options, mobile platforms, and low-bandwidth delivery.

The Knowledge-Action Gap – While threat awareness is high (86.8%), secure practices like incident reporting remain low (41.5%). This gap requires competency-based education, not just awareness. Higher embedded practice ($M = 3.42$) versus coping ($M = 3.19$) suggests training should emphasize scenario-based response confidence.

Conclusion and Recommendations

Conclusion – This study concludes that specialized cyber-security education significantly contributes to healthcare workforce resilience in Nigeria, explaining 18% of the variance. However, current provision is inadequate – 43.4% lack formal training despite a 47% annual rise in cyber-attacks.

Effectiveness varies by approach: role-based and interactive training substantially outperform generic annual awareness and passive modalities. Clinical staff exhibit the lowest resilience, highlighting the need for workflow-integrated training. Organizational support critically moderates outcomes, while unique barriers – time constraints, irrelevant content, and poor infrastructure – demand context-specific solutions.

Despite challenges, Nigerian healthcare workers demonstrate moderate embedded practice, providing a foundation for improvement. Ultimately, developing a resilient workforce requires evidence-based, role-specific, and interactive education delivered within supportive organizational contexts.

The following recommendations were made as an actionable roadmap to enhance cyber-security workforce development in alignment with the Nigeria Data Protection Act and national health workforce initiatives.

1. Mandate Role-Based Cyber-security Training for All Healthcare Professionals – Given that role-based training produced significantly higher resilience (M = 3.89) than generic annual awareness training (M = 3.31), and clinical staff scored lowest (M = 3.28), the Federal Ministry of Health should mandate differentiated, role-specific training. Clinical staff training must be integrated into workflows and framed around patient safety; technical staff require deeper technical training; administrative staff need emphasis on data protection compliance.
2. Replace Passive Training with Interactive Modalities – Since interactive training (M = 3.71) significantly outperformed passive training (M = 3.28), healthcare organizations must replace passive video-based annual training with quarterly phishing simulations, gamified micro learning modules, and scenario-based workshops delivered in 5-10 minute segments accessible via mobile devices. This addresses the barrier of irrelevant content identified by 52% of respondents.
3. Establish Protected Training Time and Leadership Accountability – With time constraints identified as the primary barrier by 67% of respondents, hospital management must formally allocate protected time for cyber-security education within work schedules. Chief Medical Directors should be held accountable for staff training completion, with cyber-security performance incorporated into annual departmental evaluations. Leaders must visibly model security behaviours.
4. Address Infrastructure Deficits Through Targeted Government Funding – Given that 48.3% identified inadequate infrastructure as a major barrier and 43.4% lack formal training despite the Nigeria Data Protection Act, the Federal Government should allocate dedicated funding to public healthcare institutions for reliable internet connectivity, updated hardware, and mobile-friendly offline training platforms, particularly for rural and under-resourced facilities.
5. Launch a National Cyber-security Awareness Campaign Framed Around Patient Safety– Building on the finding that only 41.5% report suspicious incidents, the National Orientation Agency and Federal Ministry of Health should launch a sustained national campaign using radio, television, social media, and hospital posters to frame cyber-security as essential to patient safety, emphasizing that reporting incidents protects patients and that security is a shared professional responsibility.

References

Aboh, F., Ngele, E., Okom, E., & Amoke, P. (2025). From scholars to scammers: Analysing the impact of cybercrime glamorisation on the educational development of Nigerian youths and its implications for national development. *Educational Advancement and Development Journal*, *1*(2), 212-223.

Adebayo, T. O., & Ogunleye, O. O. (2024). Cybersecurity awareness and practices among healthcare professionals in Nigerian tertiary hospitals. *Nigerian Journal of Health Informatics*, *8*(1), 34-48.

American Psychological Association. (2020). *Publication manual of the American Psychological Association* (7th ed.). https://doi.org/10.1037/0000165-000

Anas, A., Idowu, B., Okorie, E., & Okeji, M. (2025). Cybersecurity awareness among radiography teachers in Africa and its potential impact in the digital age of medicine. *BMC Medical Education*, *25*, 1219. https://doi.org/10.1186/s12909-025-07755-x

Andersen in Nigeria. (2024). *Cybersecurity risks in healthcare: Addressing Africa's digital health vulnerabilities*. https://ng.andersen.com/cybersecurity-risks-in-healthcare-addressing-africas-digital-health-vulnerabilities/

Blek, T., Mäkelä, J., & Niskakangas, J. (2025). Improving cybersecurity competence in healthcare. *JAMK University of Applied Sciences*. https://www.jamk.fi/en/project/kyberturvallisuusosaamisen-kasvattaminen-sosiaali-ja-terveysalalla

BMC Medical Informatics and Decision Making. (2025). Digital health data security practices among health professionals in low-resource settings: Cross-sectional study in Amhara Region, Ethiopia. *BMC Medical Informatics and Decision Making*, *25*(60). https://doi.org/10.1186/s12911-025-02902-2

BMC Pregnancy and Childbirth. (2024). Map of Nigeria highlighting selected tertiary hospital nurseries in the six geopolitical zones. *BMC Pregnancy and Childbirth*. https://bmcpregnancychildbirth.biomedcentral.com/

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

Dogiye, E. L., Adebisi, A. A., & Biobelemeye, G. G. (2025). Assessing data integrity and security in healthcare information management practice. *International Journal of Health Research and Information Management*, *6*(2), 45-58.

Federal Ministry of Health and Social Welfare, Nigeria. (2025). *FG partners with Achievers University, FMC Owo to boost medical training, tackle health workforce shortage*. https://health.gov.ng/fg-partners-with-achievers-university-fmc-owo-to-boost-medical-training-tackle-health-workforce-shortage/

Federal Ministry of Health, Nigeria. (2024). *Healthcare workforce development strategy 2024-2028*. https://health.gov.ng/workforce-development-strategy-2024/

Hore, K., O'Donnell, C., & McMenamin, J. (2024). Cybersecurity and critical care staff: A mixed methods study. *International Journal of Medical Informatics*, *185*, 105-112. https://doi.org/10.1016/j.ijmedinf.2024.105112

IEEE Symposium on Security and Privacy. (2025). Understanding the efficacy of phishing training in practice. In *2025 IEEE Symposium on Security and Privacy (SP)*. IEEE. https://doi.org/10.1109/SP.2025.00045

NITDA. (2023). *Nigeria Data Protection Act, 2023: Implementation guidelines for healthcare sector*. National Information Technology Development Agency. https://nitda.gov.ng/nigeria-data-protection-act-2023/

NIH. (2025). How different mixed-mode data collection approaches impact response rates and provision of biomeasure samples. *Public Opinion Quarterly*, *89*(2), 245-269. https://doi.org/10.1093/poq/nfaf022

Oisakede, E. O., & Odion, C. I. (2025). The role of cybersecurity education in Nigeria's healthcare sector. *Nigerian Medical Journal*, *66*(2), 45-58.

Okonkwo, C. C., & Nwankwo, O. C. (2024). Workforce resilience in Nigerian healthcare: A multi-dimensional approach. *Journal of Health Administration and Policy*, *12*(3), 112-128.

PMC. (2024). Cybersecurity interventions in health care organizations in low- and middle-income countries: Scoping review. *Journal of Medical Internet Research*, *26*, e47311. https://doi.org/10.2196/47311

Punch Newspapers. (2025, September 17). AI-powered cyber threats put healthcare systems at risk. *Healthwise*. https://healthwise.punchng.com/ai-powered-cyber-threats-put-healthcare-systems-at-risk-report/

The Guardian Nigeria News. (2024). *UCH CMD calls for deployment of apt resources to achieve healthcare digitalisation*. https://m.guardian.ng/uch-cmd-calls-for-deployment-of-apt-resources-to-achieve-healthcare-digitalisation/

The Sun Nigeria. (2024). *Tinubu approves immediate upgrade of UNN teaching hospital, 15 other health infrastructures nationwide*. https://thesun.ng/tinubu-approves-immediate-upgrade-of-unn-teaching-hospital-15-other-health-infrastructures-nationwide/

U.S. Department of Health and Human Services. (2024). *2023 healthcare data breach report*. Office for Civil Rights. https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html

University of Nigeria Teaching Hospital. (2024). *FASTCARE TELECLINIC (VIRTUAL CONSULTATION) NOW IN USE IN UNTH*. https://unth.edu.ng/fast-care-teleclinic-virtual-consultation-now-in-use-in-unth/

Waddell, M. (2024). Human factors in cybersecurity: Designing an effective cybersecurity education program for healthcare staff. *Healthcare Management Forum*, *37*(1), 13-16. https://doi.org/10.1177/08404704231207829

World Health Organization, Regional Office for Africa. (2025, March 13). *Empowering a new generation to lead healthcare change initiatives in Nigeria*. https://www.afro.who.int/countries/nigeria/news/empowering-new-generation-lead-healthcare-change-initiatives-nigeria