World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(RESEARCH ARTICLE)

Check for updates

Neutralization Theory-Based Model for the alleviation of Shadow IT-Induced security threats

Adinda William Odindo *, Silvance Abeka and Joshua Agola

Jaramogi Oginga Odinga University of Science and Technology, Bondo, Kenya.

World Journal of Advanced Engineering Technology and Sciences, 2025, 16(03), 088–101

Publication history: Received on 18 July 2025; revised on 03 September 2025; accepted on 05 September 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.16.3.1306

Abstract

Normally, employees bypass security measures to meet productivity goals, inadvertently creating significant cybersecurity risks. This is because they are increasingly reliant on digital tools and cloud-based workflows. Shadow IT is categorized as either a software or hardware utilized by either a department or an individual in an organization without the knowledge of the central IT unit. Institutions deploy DLP, NIDS, EDR, Zero Trust, and CASBs to monitor unauthorized data/device activities, complemented by Models like ISO 27001 and COBIT for governance. However, these struggle with rapid shadow IT adoption due to user resistance, high costs, and inability to fully cover personal devices or decentralized workflows. Regulatory mandates enforce compliance but face gaps from bureaucratic delays and evolving threats. Agile governance integrates grassroots tools into innovation pipelines and emerging risks like Generative Artificial Intelligence data leaks and quantum-vulnerable cryptography require specialized solutions. Yet, resource constraints and dynamic threats persist, necessitating real-time monitoring and behavioral incentives. This study aimed to develop a Neutralization Theory-Based Model for mitigation of Shadow IT-Induced vulnerabilities. The entire population included 150 staff from various departments within ICT Authority, Kenya. The sampling was done using Yamane's formula, yielding 110 respondents. The data was collected using an online questionnaire on google forms, whose link was shared to the 110 respondents. Cronbach's Alpha was deployed for assessment of reliability of the research tool. On the other hand, validity was tested by piloting within the security department. The obtained data was first coded on the five Likert scale prior to being fed to the SPSS software. The analysis included the computation of frequencies, percentages, multilinear regression analysis of variance and model fit tests. The results indicated that among the nine factors studied (Authorization, Role-based Access, Filtering, Logging and Auditing, Security Policies, Education and Training, Zero Trust Architecture, AI Governance, Crypto-Agility), seven had a significant positive impact on reducing Shadow IT-induced vulnerabilities. The most influential factor is AI Governance (with the highest beta of 0.312), followed by Crypto-Agility beta=0.205) and Authorization (beta=0.195). Two factors (Filtering and Security Policies) did not show a statistically significant impact in this model leading to their automatic elimination from the attuned model. AI Governance and Crypto-Agility demonstrated the strongest direct impact on reducing vulnerabilities. This directly addresses critical risks: GenAI data leakage and future quantum attacks on deprecated cryptography in shadow code. Centralized governance prevents sensitive data exposure via unauthorized AI tools, while crypto-agility mitigates long-term supply chain risks in unsanctioned scripts. Subsequently we should enforce dynamic Authorization controls integrated with Zero Trust Architecture at Policy Enforcement Points. Apply micro-segmentation specifically to isolate shadow IoT/legacy systems and enforce Role-Based Access Controls based on continuous risk assessment, not static roles. Utilize CASB/SSPM tools for real-time SaaS authorization checks.

Keywords: Neutralization Theory; Shadow IT; Role-Based Access; Generative Artificial Intelligence; Authorization; Logging and Auditing

* Corresponding author: Adinda William Odindo

1. Introduction

Shadow IT emerges when employees adopt unauthorized tools to address gaps left by rigid, enterprise-sanctioned systems like ERP platforms, which often fail to meet user needs due to unreliability, inflexibility, poor usability, or misalignment with workflows (Kopper et al., 2020; Horner et al., 2021). Dissatisfaction with centralized IT solutions drives users toward accessible alternatives, such as cloud services, SaaS applications, personal devices, or self-developed tools, enabled by the proliferation of consumer-grade technologies (e.g., smartphones, low-code platforms) that democratize IT creation (Walter Busch et al., 2022; Ghobadi and Mathiassen, 2023). In spite of its positive contributions to technological advancements, Shadow IT poses increased risks to employees through old software, low encryption and improper data backup trends. Widespread non-compliant tools utilizing Excel exports, SQL databases, and the personal devices turned into servers lack centralized administration, making them vulnerable to malware capture and uneven security practices (Orr et al., 2022; Abbas and Algal, 2021).

Neutralization Theory describes the portion of why the subjects belittle their misconduct by denying the corpus of moral beliefs in five methods including denial of responsibility, denial of injury, denial of the victim, condemnation of condemners and appeal to higher loyalties. Having developed in criminology, it has since been used in other fields such as cybersecurity and IT, where users rationalize breaking policies as either minimizing the harm or need to blame it on others (Altamimi et al., 2020; Ogedengbe et al., 2023). For instance, criminals may use self-defense to remove guilt similarly to how employees rationalize the usage of Shadow IT by saying they need this urgently or the official systems are not effective (Altamimi et al., 2020).

Recent research encompasses the usage of neutralization theory to IT which has illustrated the rationale with which users endorse Shadow IT. According to NURFITRIANSYAH et al. (2023), the situation is similar in Indonesian universities where employees operate Shadow IT because of familiarity with it and dissatisfaction with institutional tools, using such strategies as appeal to higher loyalties (more productivity than compliance), or condemnation to the condemners (the fault of IT departments, in allowing inflexible systems). In the same manner, Md Radzi and Ariffin (2023) note that the IT personnel transfer the blame of security incidents onto users, and the latter rationalize the unauthorized used instruments by denying harm (e.g., by supposing that the cloud services are safe). These analyses highlight the importance of neutralization in supporting Shadow IT through constructing it as either needed, harmless, or unavoidable (Ogedengbe et al., 2023).

In this paper, we model Shadow IT to neutralization strategies with particular behaviors in the work environment. For instance, Authorization (Denial of Responsibility), Role Based Access (Denial of Injury), Filtering (Denial of Victim), Logging and Auditing (Condemnation of Condemners) and finally, Security Policies (Appeal to Higher Loyalties). The specific contributions of this paper include the following:

- To investigate vulnerabilities and other security threats associated with Shadow IT
- To study the neutralization theory applicability in the cyber security domain
- To develop a neutralization theory-based model for mitigation of shadow IT induced vulnerabilities
- We carried out extensive evaluation of the developed model through multilinear regression analysis, analysis of variance and statistical model fits. The results indicated that there was a strong a positive correlation between authorization, Authorization, Role-based Access, Filtering, Logging and Auditing, Zero Trust Architecture, AI Governance, Crypto-Agility and the status of shadow IT vulnerabilities

The rest of this paper is structured as follows: Section 2 presents the related works while section 3 describes the methodology adopted to achieve the laid down objectives. On the other hand, Section 4 presents the obtained results, while section 5 discusses these results. Towards the end of this paper, section 6 provides the conclusion as well as future research scopes

2. Related works

To mitigate Shadow IT risks, institutions deploy Models like Data Loss Prevention (DLP), Network Intrusion Detection Systems (NIDS), and Endpoint Detection and Response (EDR) tools to monitor unauthorized data transfers and device activities (Abbas and Algal, 2021; Bongiovanni, 2019). Regulatory measures, such as Kenya's Data Protection Act (DPA) 2019 and the National Cybersecurity Strategy, mandate compliance with data privacy and cybersecurity standards, particularly in STEM universities handling sensitive research and student data. However, these Models struggle to keep pace with the rapid adoption of unauthorized cloud services, self-installed software, and personal devices, which remain prevalent due to gaps in institutional IT offerings (Selma Gomez et al., 2024; Trang, N. 2023). To mitigate this risk

properly, a multi-level strategy is necessary: preventing connection to the network, the use of high-quality passwords, and the security profile of the Shadow IT tools to evaluate the degree of vulnerability (Orr et al., 2022). It is essential to provide staff, and students with training programs that improve IT literacy and advanced threat awareness, and keep balance between innovation and compliance (Abbas and Alghail, 2021). But the kinetic essence of Shadow IT including unauthorized cloud services with no exit plans or encryption presents a problem to institutions. Active governance, real-time reporting instruments, and the agile policy governance are necessary to handle evolving cybersecurity threats without compromising on academic productivity (Selma Gomez et al., 2024; Trang, N. 2023).

In order to address these risks, such Models as Zero Trust Architecture and Cloud Access Security Brokers (CASBs) play a vital role in terms of ensuring compliance and protection of data (Abbas and Alghail, 2021). On the same note, solutions like Endpoint Detection and Response (EDR) or Security Information and Event Management (SIEM) offer insights into unauthorized IT activities, but their adoption is hampered by the issue of resistance (by users), as well as high costs (Fursenau, and Rothe, 2014, Bongiovanni, 2019). In decentralized conditions, such Models are especially important because hybrid work Models increase the dependence on unapproved tools (Ghobadi and Mathiassen, 2023). Although shadow IT leads to the innovation by users, its management is an exercise in balancing creativity and compliance. Models such as Software Asset Management (SAM) and User and Entity Behavior Analytics (UEBA) provide support to monitor the usage according to Silic and Back (2014), but these are not easy to gain a buy-in by an employee. Bongiovanni (2019) emphasizes the importance of training and policy governance in the organizations as the means of risk mitigation but implementation becomes complicated due to the factors of resource scarcity and constant threat changes. Adoption of modern trends involves the recommendations to incorporate shadow IT into ideas pipelines instead of trying to limit it and transform the grassroot-created solutions into approved tools through agile governance (Walterbusch et al., 2022). Such two-pronged approach that capitalized on the speed of shadow IT deployments in addition to imposing security measures such as Zero Trust is how organizations can meet the unmet needs of users without sacrificing security (Kretschmer et al., 2022; Selma Gomez et al., 2024).

Modern research focuses on an all-embracing approach to mitigation that demands the combination of technology and governance, alongside cultural approaches (Gartner, 2024). Legacy solutions of purely technical controls are deficient to solve causes of the problem such as the bureaucratic process of procurements or agility requirements of the employees. Besides, risk-alignment modeling solutions like Gartner IT Shadow Continuum Model suggest a balanced alignment of risks and innovation and customize the key principles of CIS Critical Security Controls v8 and other security frameworks to the modern hybrid environment (Gartner, 2024; CIS, 2023; NIST, 2021). Discovery and prevention technologies form the first pillar of defense. Automated asset discovery via Cloud Access Security Brokers (CASB) and SaaS Security Posture Management (SSPM) tools enables real-time visibility into shadow SaaS usage, while network traffic analysis and eBPF-based observability detect anomalous connections in cloud-native workloads (Gartner, 2023; IEEE, 2023). Prevention leverages Zero Trust Architecture (ZTA) per deploying Policy Enforcement Points to block unauthorized access and micro segmentation to isolate shadow IoT devices. Complementary technical guardrails include DLP (Microsoft Purview) for data exfiltration, SBOM scanning (Snyk) for supply chain risks, and Unified Endpoint Management (Intune) to control local scripts (NIST, 2023; MITRE, 2024).

Governance and cultural strategies are equally critical. Standardized Models like ISO/IEC 27001:2022 (asset management), COBIT APO12.05 (risk-based approvals), and CIS Control 1 (continuous inventory) formalize accountability for shadow assets (ISACA, 2023). Policy templates such as Acceptable Use Policies restricting unsanctioned GenAI and Automation Governance Policies mandating peer reviews operationalize compliance (Cloud Security Alliance, 2024). Culturally, sanctioned alternatives and behavioral programs reduce shadow IT adoption by addressing employee needs for agility. Amnesty initiatives and innovation-focused KPIs further foster trust, increasing shadow tool reporting (Forrester, 2024; Deloitte, 2023). Emerging threats necessitate specialized mitigations. The proliferation of generative AI shadow tools risks intellectual property leakage, countered by LLM gateways (Palo Alto AI Security) for data masking and NIST AI RMF-aligned impact assessments (OWASP, 2024; NIST, 2023). Quantum-vulnerable shadow systems using deprecated cryptography are mitigated via crypto-discovery tools (Venafi) and post-quantum standards (NIST FIPS 203/204) (NIST, 2023).

3. Methodology

This section covers the methodology, including the research design that was selected and the rationale behind it to examine the research problem. In addition, research population, research sample size, sample technique, research instruments, methods for gathering information, and the data analysis, reliability, and validation are covered here as well. It also detailed the methodical process used to develop a Neutralization theory-based Model for mitigating shadow IT-induced vulnerabilities in organizations.

3.1. Research Design

The study employed quantitative methodology. Shadow IT concepts, forms, Models, adoption techniques and the potential benefits and dangers investigated by statistically analyzing survey data from the prospective questionnaire responses.

3.2. Target Population of the Study

The ICT Authority, a State Corporation established under CAP 446 within the Ministry of Information Communication and the Digital Economy whose broad mandate includes but not limited to enforcing ICT standards and maintaining secure ICT infrastructure and systems in Government made up the study population. Other like-minded industry players or stakeholders who showed interest were also engaged, either directly or indirectly for varied opinions to count and for validation purposes at the end of the study. This aimed to widen the spectrum and diversity of opinion within the areas of specialization since some were law makers or even contractors whom ICT Authority engaged in various projects.

3.3. Sampling Techniques and Sample Size

Purposive sampling was employed in this research in order to capture feedback from varied experts with different specializations from different departments regarding the subject matter. This made it possible to assume that the sample was representative of a wide range of viewpoints and experiences, but pertinent to the study by choosing participants according to defined criteria.

At ICT Authority Headquarters, there are approximately 150 staff spread across 5 departments. The research therefore employs Yamane's formula for sampling purposes as demonstrated below through a proportionate stratified sampling design

Assuming a 95% confidence level and a maximum variability (p = 0.5). The minimum sample size required can be established as:

$$n = \frac{N}{(1+N(e^2))} \qquad Equation\ (1)$$

Were

- n= sample size
- N = population size
- e = margin of error (expressed as a decimal, e.g., 5% = 0.05)

Calculation for N=150

Assume a 5% margin of error (e=0.05):

n=150/ (1+150(0.052)) ≈ 109.09

Round up to the nearest whole number gives the required sample size of 110.

3.4. Data Collection

The researcher opted for a questionnaire as a tool because of its objectivity since the questions are presented online and there is no opportunity for interviewers' bias. The questionnaire design was informed by insights from the literature review and research objectives. It included sections aimed at understanding core issues with Shadow IT adoption, evaluation of existing techniques for threats mitigation and gathering input on the proposed Model development and validation process.

3.4.1. Data collection procedure

Data collection occurred through electronic distribution of the survey questionnaire to selected participants. This was clearly achieved through google forms after obtaining the necessary documentations and approvals from the Board of Post Graduate Studies (BPS), NACOSTI and the ERC for Ethics Review. Level of confidentiality and the purpose for the

data collection was thoroughly articulated before the respondents could confide and give proper feedback through questionnaires.

3.4.2. Reliability of the research instruments

According to (Atheros, 2016), reliability is the extent to which a research tool consistently produces steady results repeatedly. The reliability of the survey instrument was assessed using Cronbach's Alpha, which is a measure of internal consistency among the items. Cronbach's alpha coefficient was used in the study to assess the survey items' internal consistency to guarantee the validity of my findings. Furthermore, content validity was used to demonstrate the validity of the study instruments and made sure they appropriately assessed the target components.

The Cronbach's Alpha value was 0.905 from the 9 possible variables as indicated in the Table 3.1, which showed that the variables were sufficiently consistent, confirming that results were reliable.

3.4.3. Validity of the research instrument

In this study, the validity of the research instruments was measured through establishing face validity by engaging captains of industries in the same niche that I knew. This enabled me to share a preview of what I wanted to achieve with them to help refine the questionnaire and mode of delivery of the same to avoid null inputs and faster feedback and I believe that this incorporates both empirical and theoretical evidences.

3.4.4. Data analysis

Data analysis involved descriptive statistics through generation, and validation of interpretations, formulation inferences and drawing relevant conclusions using statistical parameters to identify trends and patterns in neutralization theory-based Shadow IT perspective and Current techniques employed to mitigate on the potential threat landscape.

To analyse the relationship between various factors and the neutralization theory perspective of Shadow IT, regression analysis and correlation was employed after coding and feeding the Data in SPSS then finding the p-value and z-scores. The inferences drawn from the analysis and interpretation pointed to a Neutralization Theory-oriented model for mitigation of Shadow IT-induced vulnerabilities. The regression model is defined by the following equation:

$$Y = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3 + \beta_4 x_4 + \beta_5 x_5 + \beta_6 x_6 + \beta_7 x_7 + \beta_8 x_8 + \beta_9 x_9 \qquad Equation\ (2)$$

Were

- Y=Vulnerability Mitigation
- $\beta 0$=Constant
- $x1$=Filtering
- $x2$=Authorization
- $x3$=Role-Based Access
- $x4$=Security Policies
- $x5$=Logging and Auditing
- $x6$=Education and Training
- $x7$=Zero Trust Architecture
- $x8$=AI Governance
- x9=Crypto-Agility

4. Results

As already stated above, a total of 150 questionnaires were issued to respondents and 110 questionnaire feedbacks were received, translating to 73.3% of the response rate. A response rate of 50% is adequate and a response rate that is greater than 70% is considered to be very good, Mugenda (2003). The questionnaire comprised of 5 sections, that is; Demographic data, threat landscape through Neutralization theory, mitigation strategies through techniques, and intervening variables for moderation and finally, a vulnerability mitigation model.

4.1. Demographic Data

This section provides data about the gender of respondents, age group distribution, years of service and the specific roles in the Organization. The specific details are described below.

4.1.1. Gender of Respondents

The respondents were asked to indicate their gender from male, female or other. Distribution of Respondents in terms of gender emerged as 65(59.1%) for Male and 45(40.9%) for Female out of all the 110 respondents as shown below in Table 1 and Figure 1.

Table 1 Gender Frequency

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	65	59.1	59.1	59.1
	Female	45	40.9	40.9	100.0
	Total	110	100.0	100.0	

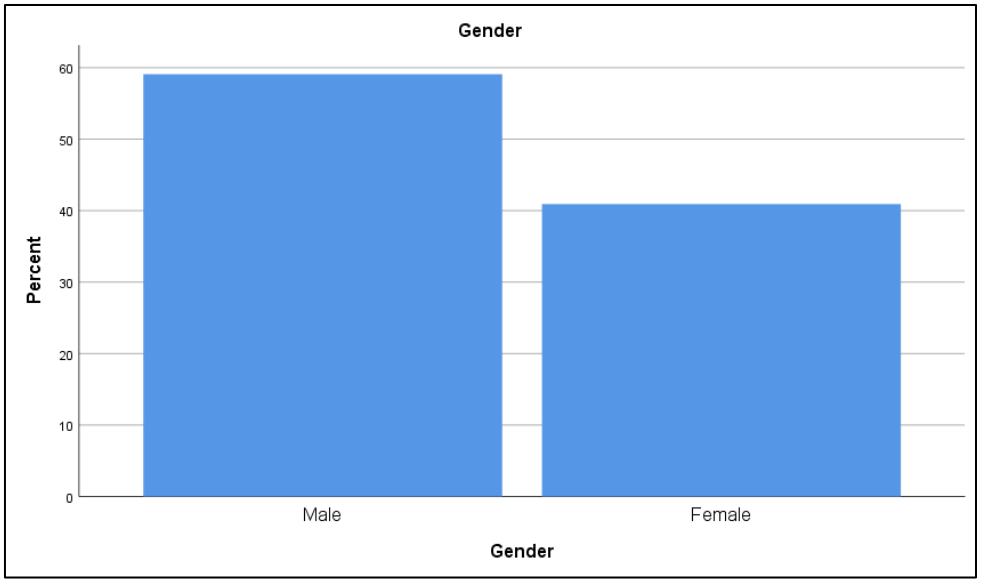

Figure 1 Gender distribution

4.1.2. Age Group Distribution

The respondents were asked to select their age from the following ranges in years; Below 25, 25-43, 35-44, 45-54, 55 and above. The results indicated that the age bracket of employees between 25 to 34 years of age had the highest representation of 56(50.9%) while those who fell at 55 and above years of age were the least represented at 3(2.7%). Those who were below 25 years of age frequented at 11(10.0%), those between the ages of 35 to 44 were at 33(30.0%) and finally, those between 45 to 54 years of age were 7, representing a 6.4% of the valid respondents as indicated below in Table 2 and Figure 2.

Table 2 Age-Group Frequency

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Below 25	11	10.0	10.0	10.0
	25-34	56	50.9	50.9	60.9
	35-44	33	30.0	30.0	90.9
	45-54	7	6.4	6.4	97.3
	55 and above	3	2.7	2.7	100.0
	Total	110	100.0	100.0	

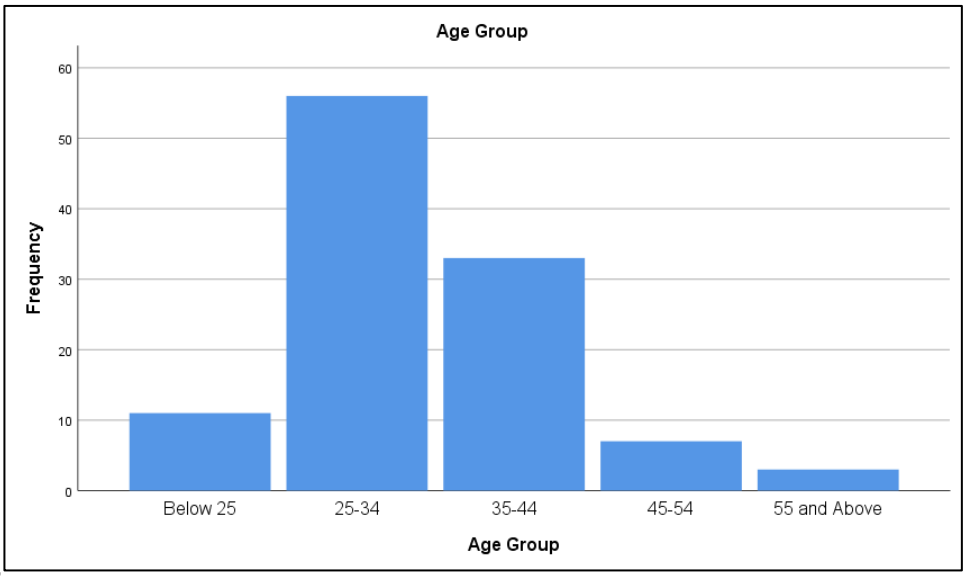

Figure 2 Age group distribution

4.1.3. Years of Service

The respondents were asked to indicate their years of experience from the following ranges in years; Below 3;4-6;7-9;10-12; Above 12. The results showed that the majority of employees had between 4 to 6 years of service at the Authority representing 58/110(52.7%) while only 4 out of 110 employees representing a 3.6% had lasted in the organization for more than 12 years. Those who were below 3 years old in the organization made up a total of 12(10.9%), those between 7 to 9 years of service were 30(27.3%). Finally, those with between 10 to 12 years of service were found to be 6 representing a total of 5.5% of the respondents as shown below in Table 3 and Figure 3.

Table 3 Years of Service Frequency

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Below 3	12	10.9	10.9	10.9
	4-6	58	52.7	52.7	63.6
	7-9	30	27.3	27.3	90.9
	10-12	6	5.5	5.5	96.4
	Above 12	4	3.6	3.6	100.0
	Total	110	100.0	100.0	

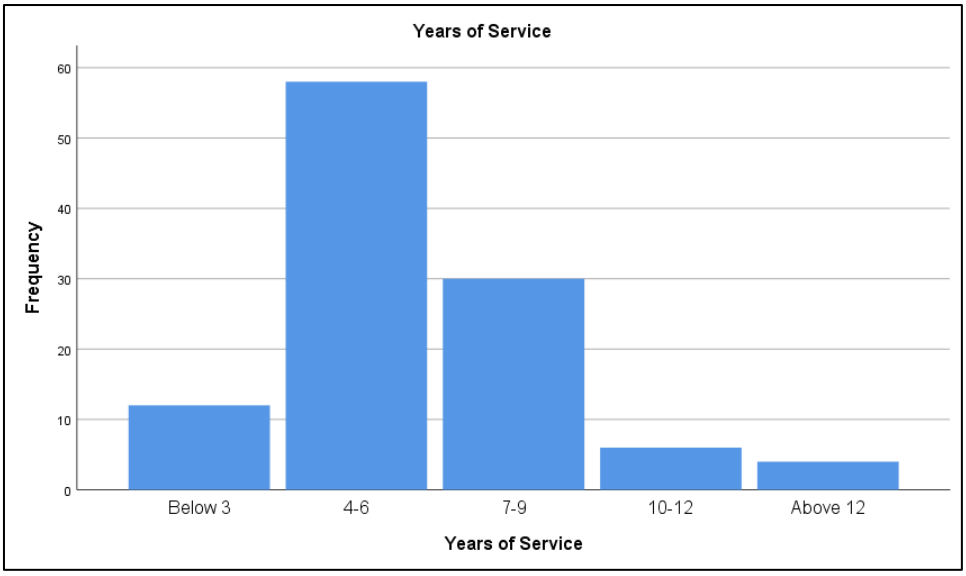

Figure 3 Work experience distribution

4.1.4. Role in the Organization

The respondents were requested to select their respective roles in the organization from the following options.; ICT Officer, Data Centre Staff, Incubation Officers, Security Analysts and NOC Engineers. The results indicated that ICT Officers had 11(10.0%), Data Centre Staff 24(21.8%), Incubation Officers 10(9.1%), Security Analysts 42(38.2%) and finally, the NOC Engineers constituted 23 staff representing (20.9%) as shown in Table 4 and Figure 4 below.

Table 4 Role in organization frequency

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ICT Officer	11	10.0	10.0	10.0
	Data Center Staff	24	21.8	21.8	31.8
	Incubation Officer	10	9.1	9.1	40.9
	Security Analyst	42	38.2	38.2	79.1
	NOC Engineer	23	20.9	20.9	100.0
	Total	110	100.0	100.0	

Figure 4 Designations distribution

The proposed model was broken down into 3 major categories, the independent variables which fell into both the Neutralization theory techniques as well as the mitigation techniques all in the name of predictor variables, which were then moderated by two intervening variables of organizational behaviour and cost implications to see how they would influence the vulnerability mitigation model.

4.1.5. Neutralization Theory

This theory had five constructs in the name of Authorization (Denial of Responsibility), Role Based Access (Denial of Injury), Filtering (Denial of Victim), Logging and Auditing (Condemnation of Condemners) and finally, Security Policies (Appeal to Higher Loyalties).

The respondents were asked to indicate their level of satisfaction with such approaches in a bid to achieve a vulnerability mitigation model and the responses were summarized as shown below for further analysis and interpretation

4.1.6. Mitigation Techniques

A total of 4 constructs which equally formed part of the independent variables namely; Education and Training, Zero Trust Architecture, Artificial Intelligence and the most recent Crypto-Agility, a data encryption response to cryptographic threats. The respondents were asked to confirm how such techniques were able to ensure a vulnerability mitigation and a summary of the responses were captured as shown below in figure 4.

4.1.7. Moderators

To moderate the effects of the 9 independent variables, the research engaged two intervening variables, namely; Cost implications and the Organizational Behavior. The respondents were requested to confirm whether such factors were influencing a vulnerability mitigation model and the below is the summary of the resultant feedback as shown in Table 5.

Table 5 Multilinear regression coefficient

Coefficients									
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B		Collinearity Statistics	
		B	Std. Error	Beta			Lower Bound	Upper Bound	Tolerance	VIF
1	(Constant)	-1.385	.149		-9.300	.000	-1.680	-1.089		
	Filtering	-.067	.078	-.042	-.855	.395	-.222	.088	.486	2.057
	Authorization	.271	.070	.195	3.888	.000	.133	.409	.469	2.132
	Role-Based Access	.165	.063	.114	2.631	.010	.041	.289	.632	1.583
	Security Policies	-.034	.066	-.025	-.524	.601	-.164	.096	.512	1.952
	Logging and Auditing	.227	.068	.176	3.340	.001	.092	.362	.426	2.348
	Education and Training	.167	.074	.122	2.270	.025	.021	.314	.408	2.450
	Zero Trust Architecture	.185	.074	.125	2.487	.015	.037	.333	.466	2.144
	AI Governance	.363	.064	.312	5.651	.000	.235	.490	.388	2.579
	Crypto-Agility	.277	.068	.205	4.091	.000	.143	.411	.472	2.118

Dependent Variable: Reduced Shadow IT-Induced Vulnerabilities

The following regression equation can be derived based on the coefficient of correlation in Table 5.

$Y = \beta 0 + \beta 1x1 + \beta 2x2 + \beta 3x3 + \beta 4x4 + \beta 5x5 + \beta 6x6 + \beta 7x7 + \beta 8x8 + \beta 9x9$ *Equation* (*3*)

$Y = -1.385 + 0.271X_2 + 0.165X_3 + 0.227X_5 + 0.1.67X_6 + 0.185X_7 + 0.363X_8 + 0.277X_9$ *Equation* (*4*)

The table of coefficients shows the impact of each independent variable on the dependent variable, while holding other variables constant. Looking at the "Standardized Coefficients (Beta)" to compare the relative importance of each variable. The higher the absolute value of Beta, the stronger the effect. In terms of significance, all the 7 predictors with ($p < 0.05$) as stated below are statistically significant;

- Authorization: Beta = 0.195, p = 0.000 -> Significant positive impact.
- Role-Based Access: Beta = 0.114, p = 0.010 -> Significant positive impact.
- Logging and Auditing: Beta = 0.176, p = 0.001 -> Significant positive impact.
- Education and Training: Beta = 0.122, p = 0.025 -> Significant positive impact.
- Zero Trust Architecture: Beta = 0.125, p = 0.015 -> Significant positive impact.
- AI Governance: Beta = 0.312, p = 0.000 -> Significant positive impact (strongest).
- Crypto-Agility: Beta = 0.205, p = 0.000 -> Significant positive impact.

However, the following variables were not significant ($p > 0.05$)

- Filtering: Beta = -0.042, p = 0.395 -> Not significant.
- Security Policies: Beta = -0.025, p = 0.601 -> Not significant.

The VIF (Variance Inflation Factor) values are all below 5 (ranging from 1.583 to 2.579), which is acceptable (VIF < 10 is generally considered non-problematic). This indicates that multicollinearity is not a severe issue.

Among the nine factors studied, seven have a significant positive impact on reducing Shadow IT-induced vulnerabilities. The most influential factor is AI Governance (with the highest beta of 0.312), followed by Crypto-Agility (beta=0.205) and Authorization (beta=0.195).

Two factors (Filtering and Security Policies) did not show a statistically significant impact in this model. This might be because their effect is captured by other variables or they are not as directly impactful in this context definitely eliminating them from the model leading to the attuned model in Figure 4.9 below.

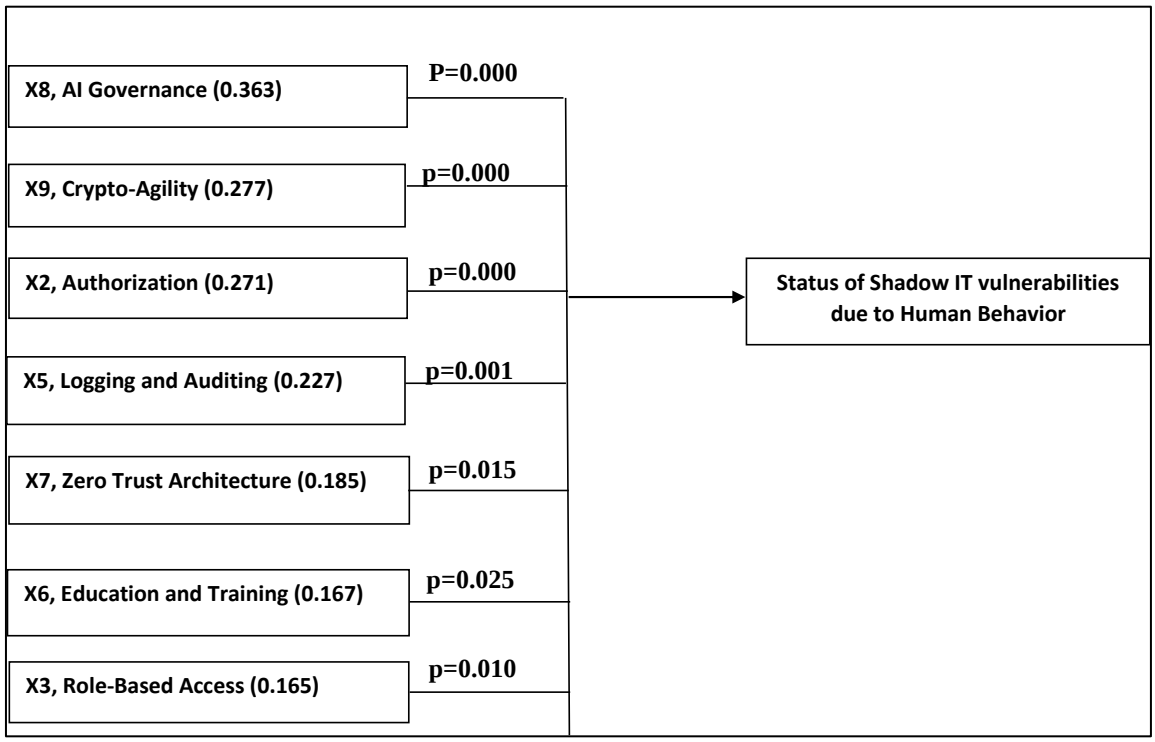

Figure 5 The Attuned Model

5. Discussion

Based on the analysis we carried out, R (Multiple Correlation Coefficient) = 0.939: This indicates a very strong positive relationship between the independent variables and the dependent variable. Additionally, at 95% confidence interval, it shows a good model fit: F (9,100) = 82.67, P<0.005, Adj R2 = 0.871 and the coefficient of determination R2 = 0.882 (0.882x100 = 88.2%), proportion of variability in the outcome variable accounted for by the predictor variable. Adjusted R Square = 0.871: This adjusts the R Square for the number of predictors and is still very high, indicating the model is robust. Std. Error of the Estimate = 0.415: This is the average error in predicting the dependent variable. The lower the value, the better the model's predictions. Durbin-Watson = 1.603: This tests for autocorrelation of residuals. A value around 1.5 to 2.5 is generally acceptable, so 1.603 is acceptable as shown in Table 6 below.

Table 6 Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics					Durbin-Watson
					R Square Change	F Change	df1	df2	Sig. F Change	
1	.939[a]	.882	.871	.415	.882	82.669	9	100	.000	1.603
a. Predictors: (Constant), Crypto-Agility, Role-Based Access, Security Policies, Authorization, Filtering, Zero Trust Architecture, Logging and Auditing, Education and Training, AI Governance										
b. Dependent Variable: Reduced Shadow IT-Induced Vulnerabilities										

The overall model is statistically significant because the p-value (Sig.) is 0.000 (which is less than 0.05). This means that the independent variables, taken together, significantly predict the dependent variable. This is well illustrated in Table 7below.

Table 7 ANOVA

Model		Sum of Squares	DF	Mean Square	F	Sig.
1	Regression	128.189	9	14.243	82.669	.000[b]
	Residual	17.229	100	.172		
	Total	145.418	109			

Dependent Variable: Reduced Shadow IT-Induced Vulnerabilities, Predictors: (Constant), Crypto-Agility, Role-Based Access, Security Policies, Authorization, Filtering, Zero Trust Architecture, Logging and Auditing, Education and Training, AI Governance

The obtained results show strong employee agreement exists with all security practices (70-85% combined "Agree/Strongly Agree" across practices like Authorization, RBAC, Logging, Policies, Education). Employees cognitively separate agreeing with the principle of security from justifying specific violations using neutralization techniques. They endorse the policies ("Agree") but still use unauthorized tools because they neutralize the moral conflict ("I agree security is important, but I need this tool to meet my deadline/help my team"). High agreement with Authorization (76.4% Agree/SA) supports its role in countering Denial of Responsibility by forcing acknowledgment of rules. High agreement with Role-Based Access (78.2% Agree/SA) aligns with disrupting Denial of Injury by limiting access to sensitive assets. Logging and Auditing (77.3% Agree/SA) targets Condemnation of Condemners by providing objective evidence of enforcement consistency.

Practices like Authorization, RBAC, and Security Policies show very high agreement (75-83% cumulative for Agree/SA). This suggests they are well-understood and accepted, forming a solid foundation for directly countering key neutralizations (Responsibility, Injury, Loyalties). While Logging and Auditing has good agreement (77.3% Agree/SA), its higher "Disagree/Strongly Disagree" (9.1%) compared to others (mostly 5-8%) might indicate perceptions of invasiveness or inefficacy, potentially undermining its fight against Condemnation of Condemners. Filtering has the lowest "Agree/Strongly Agree" (83.6%) and highest "Neutral" (10%), suggesting it might be seen as obstructive, requiring careful implementation to avoid fueling Denial of Victim or Condemnation justifications. AI Governance shows the highest "Strongly Agree" (25.5%) but also notable "Disagree/Strongly Disagree" (10%), reflecting heightened awareness but also significant dissent or uncertainty about governance approaches. Crypto-Agility has the lowest "Strongly Agree" (14.5%) and highest "Agree" (64.5%), indicating it's accepted but perhaps not seen as critically urgent by many, posing a risk if deprecated crypto is used in shadow systems.

6. Conclusion

Human behavior was emerging as the weakest link in a security domain, prompting urgency-driven policy violations which escalate vulnerabilities and threats exposure leading to high risks and potential losses. The security challenges were mapped into neutralization theory techniques then sent out in form of practical questionnaires after obtaining all the necessary requirements to conduct research. The data was then coded in SPSS and analyzed appropriately to obtain multilinear regression results, frequency distribution and various model fits for further interpretation and decision making. Regarding the key findings of this research, modern practices like AI Governance (β=0.312) and Crypto-Agility (β=0.205) emerged as strong, novel counters to neutralization, especially in the context of evolving technologies like generative AI. These tools address new forms of rationalization and mistrust in traditional IT controls, highlighting the need to expand the theory beyond its original 1957 framework. The results transform Neutralization Theory from a purely conceptual model into a validated, adaptive tool for mitigating Shadow IT one that now incorporates behavioral insight, modern technological risks, and empirically proven controls. Theoretical Implication is that Neutralization Theory provides a valid foundation for Shadow IT mitigation when augmented with modern practices. The results validate 3 core Neutralization Theory counters (Authorization, RBAC, Logging), and refute 2 assumed counters (Filtering, Security Policies). In addition, the results indicate that employee agreement with policies doesn't prevent neutralization. In this study, we expand the theory to include AI/crypto practices as critical modern counters. This transforms Neutralization Theory from a conceptual framework into an empirically grounded model for Shadow IT mitigation. The developed findings act as a paradigm shift in shadow IT mitigation, transitioning cybersecurity from technical enforcement to behavioral transformation. By embedding AI-driven governance, cryptographic resilience, and dynamic access controls within a culture of collaboration, the model neutralizes the rationalizations fueling shadow IT. Organizations should prioritize the seven validated factors especially AI Governance and Crypto-Agility while

streamlining policies and filtering. The result is a human-centric security ecosystem: resilient, compliant, and enabling innovation without compromising productivity. As a final blueprint, the NTBM delivers a scalable model to turn human behavior from a vulnerability into an organizational strength, fulfilling this study's mandate to secure innovation while empowering the workforce to thrive. The developed model recognizes AI's potential for real-time Shadow IT management as nascent, though AI-powered CASBs (Cloud Access Security Brokers) and can auto-detect and block unauthorized apps, yet depicts minimal research on Ethical AI deployment which in the real threat with the greatest weight since AI is not bad but the intentions of the users might be malicious at times. Aligning policies with decentralized workflows. Addressing peer-driven Shadow IT adoption. Securing Bring-Your-Own-Device (BYOD) cultures in SMEs (Trang Nguyen, 2023). In summary, no holistic governance Models exist to harmonize Shadow IT's innovative potential with hybrid work security needs.

Compliance with ethical standards

Disclosure of conflict of interest

The authors declare that they hold no conflict of interest.

References

[1] Kopper, A., et al. (2020). Shadow IT and Innovation: A Double-Edged Sword. Journal of Information Technology.

[2] Horner, D., et al. (2021). User-Centric IT Dissatisfaction and the Rise of Shadow Systems. Information and Management.

[3] Walterbusch, M., et al. (2022). Cloud Adoption and Decentralized IT Practices. International Journal of Information Management.

[4] Ghobadi, S., and Mathiassen, L. (2023). Hybrid Work and Shadow IT: The Blurring Boundaries of Personal and Professional Tech. Journal of Strategic Information Systems.

[5] Orr, S. G., Bonyadi, C. J., Golaszewski, E., Sherman, A. T., Peterson, P. A., Forno, R., ... and Rodriguez, J. (2024). Shadow IT in higher education: survey and case study for cybersecurity. Cryptologia, 48(1), 26-90.

[6] Abbas, M., and Alghail, A. (2023). The impact of mobile shadow IT usage on knowledge protection: an exploratory study. VINE Journal of Information and Knowledge Management Systems, 53(4), 830-848.

[7] Abbas, M., and Alghail, A. (2023). The impact of mobile shadow IT usage on knowledge protection: an exploratory study. VINE Journal of Information and Knowledge Management Systems, 53(4), 830-848.

[8] Ogedengbe, F. A., Abdul Talib, Y. Y., and Rusly, F. H. (2024). Influence of structural factors on employee cloud shadow IT usage during COVID-19 lockdown: a strain theory perspective. Cognition, Technology and Work, 26(1), 63-81.

[9] Trang, N. (2023). Understanding Shadow IT usage intention: a view of the dual-factor model. Online Information Review.

[10] Fürstenau, D., and Rothe, H. (2014). Shadow IT systems: discerning the good and the evil.

[11] Bongiovanni, I. (2019). The least secure places in the universe? A systematic literature review on information security management in higher education. Computers and Security, 86, 350-357.

[12] Silic, M., and Back, A. (2014). Shadow IT - A view from behind the curtain. Computers and Security, 45, 274–283.

[13] Kretschmer, T., et al. (2022). Productivity vs. Compliance: Employee Trade-offs in Shadow IT Adoption. MIS Quarterly.

[14] Taherdoost, H. (2016). Validity and Reliability of the Research Instrument; How to Test the Validation of a Questionnaire/Survey in a Research. SSRN Electronic Journal.

[15] Cloud Security Alliance. (2024). Automation governance policy framework.

[16] CIS. (2023). CIS Critical Security Controls v8. Center for Internet Security.

[17] Deloitte. (2023). Cultivating trust: Behavioral strategies for cybersecurity compliance. Deloitte Insights.

[18] Forrester. (2024). The future of work: Balancing innovation and risk. Forrester Research, Inc.

[19] Gartner. (2023). Market guide for SaaS security posture management. Gartner, Inc.

[20] Gartner. (2024). IT Shadow Continuum Model: Achieving balanced alignment. Gartner, Inc.

[21] IEEE. (2023). Leveraging eBPF for cloud-native observability and security. IEEE Cloud Computing.

[22] ISACA. (2023). COBIT 2019 framework: Governance and management objectives. ISACA.

[23] MITRE. (2024). MITRE ATTandCK® for supply chain: Techniques and mitigation. The MITRE Corporation.

[24] NIST. (2021). NIST cybersecurity framework (CSF). National Institute of Standards and Technology.

[25] NIST. (2023). AI risk management framework (AI RMF 1.0). National Institute of Standards and Technology.

[26] NIST. (2023). Implementing a zero trust architecture (Special Publication 800-207A). National Institute of Standards and Technology.

[27] OWASP. (2024). OWASP top 10 for large language model applications. OWASP Foundation.

[28] Nurfitriansyah, Munir, M., Disman, D., and Dirgantari, P. (2023). Does Individual IT Experience Affect Shadow IT Usage? Empirical Evidence from Universities with Legal Entities in Indonesia. Organizacija, *56*(3), 265–277.