International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

IT End-User Training Framework for Mitigating Human-Related Internal Cybersecurity Risks: A Case Study of Uganda Coffee LTD

Musa Nsubuga[1], Ali Najib[2], David Kaketo[3], Kimera Rogers[4]

[1]Postgraduate Student, Faculty of Science and Technology, School of Postgraduate Studies and Research, Victoria University, Kampala, Uganda
[2,3]Senior Lecturer, Faculty of Science and Technology, School of Postgraduate Studies and Research, Victoria University, Kampala, Uganda
[4]Lecturer, Faculty of Science and Technology, School of Postgraduate Studies and Research, Victoria University, Kampala, Uganda

Abstract

In 2021, Uganda Coffee Ltd sustained a ransomware attack initiated through a spear-phishing email, exposing the limits of technical controls when employees are the vulnerability. Despite firewalls, intrusion detection systems, and antivirus deployment, human-related risks, including phishing susceptibility, social engineering, credential compromise, and accidental data sharing, continued to create persistent attack pathways. This study designed and proposed a targeted IT End-User Cybersecurity Training Framework to mitigate human-related internal cybersecurity risks, guided by four objectives: analyzing existing IT end-user training frameworks and their relevance to the organizational operational needs; evaluating the relationship between IT end-user training and risk mitigation; designing a tailored framework; and evaluating its expected effectiveness.

The study adopted a mixed research design drawing on two structured questionnaires, one administered to 108 employees and the other to five purposively selected key technical informants, supplemented by a secondary dataset of 1,400 phishing simulations administered across the same workforce over five years (2021–2025). Descriptive statistics and Chi-Square Tests of Independence were applied using SPSS Statistics. The study is theoretically grounded in Protection Motivation Theory (Rogers, 1975), Human Error Theory (Reason, 1990), and Socio-Technical Systems Theory (McEvoy & Kowalski, 2019).

The findings confirmed that 30% of employees were untrained or uncertain of their training status, and 42.6% had been trained at most once. The simulation data revealed a stark behavioural gap: untrained employees recorded an average phish rate of 22.1% against 7.3% for trained employees, and 91.7% of untrained employees were classified as High Risk compared to zero trained employees. A Chi-Square test confirmed the association is statistically significant at $\chi^2(4) = 99.063$, $p < 0.001$, Cramér's V = 0.677, a large effect. A statistically significant gender training gap was also identified, with male employees receiving training at 78.8% against 54.8% for female employees ($p = 0.007$). All five key informants described real cybersecurity incidents as attributed to insufficient training, including the 2021 ransomware attack origin. Between 98.1% and 100% of respondents agreed across all framework effectiveness items, with no disagreement recorded on any item.

The proposed five-phase framework, designed and drawn using draw.io, is projected to reduce the overall phish rate from 11.0% toward the 4–8% industry benchmark and eliminate High Risk classification among trained employees within 24 months. The study concludes that inclusive, mandatory, quarterly, role-differentiated training with formal appraisal integration is significantly associated with the mitigation of human-related cybersecurity risk, contributing original empirical evidence from an East African agri-commodity context.

Keywords: Cybersecurity Training, Human-Related Cybersecurity Risks, End-User Awareness, Phishing, Human Error Theory, Protection Motivation Theory, Phish Rate, Phish Report.

Introduction

This study examines the design of an IT end-user cybersecurity training framework aimed at mitigating human-related internal cybersecurity risks at Uganda Coffee LTD, a coffee trading and processing company operating within the East African agri-commodity sector.

Historical Perspective

Globally, organisational cybersecurity training has evolved from generic, one-off awareness sessions toward continuous, behaviourally grounded programmes as evidence has accumulated that human error, rather than purely technical failure, is the dominant vector for security incidents (Verizon, 2024). Landmark contributions such as Reason's (1990) Human Error Theory reframed workplace security failures as predictable and systemic rather than the result of individual negligence, prompting organisations worldwide to redesign training around role-specific error patterns rather than blanket instruction. Many organisations have since reformed their security awareness programmes, recognising that employees perform more securely when training is recurrent, contextualised, and reinforced through simulation rather than delivered as a single static event (SANS Institute, 2024).

Theoretical Perspective

The study was steered jointly by Protection Motivation Theory (Rogers, 1975), Human Error Theory (Reason, 1990), and Socio-Technical Systems Theory (McEvoy & Kowalski, 2019), supplemented by Deterrence Theory (Karami, 2025) and the Behavioural Change Model (Hweidi & Eleyan, 2022). Protection Motivation Theory explains that an employee is most likely to adopt protective security behaviour when they perceive a threat as serious and personally relevant, and believe the recommended protective action is both effective and within their capability (Sulaiman et al., 2022); this theory directly justifies the recurring, quarterly structure of the proposed framework, since a single training event produces threat appraisal that decays without reinforcement. Human Error Theory classifies errors into slips, lapses, mistakes, and violations that arise from cognitive limitations, environmental pressures, and inadequate training rather than wilful negligence (Mai & Khalid, 2025), justifying the framework's role-differentiated design. Socio-Technical Systems Theory holds that effective security interventions must align human behaviour, technical tools, and organisational culture simultaneously, since technical controls alone cannot prevent human-error-induced breaches (McEvoy & Kowalski, 2019); this theory underpins the framework's governance and appraisal-integration layer. For that reason, these theories collectively provided the behavioural, cognitive, and organisational link between IT end-user training and the mitigation of human-related cybersecurity risk in this study.

Contextual Perspective

The study was undertaken at Uganda Coffee LTD, located in Bweyogere Division, Kira Municipality, Wakiso District, Uganda. This case was selected following a real ransomware incident in 2021, initiated through a spear-phishing email, which exposed the limits of the organization's technical controls when its own employees became the point of failure. Despite firewalls, intrusion detection systems, and antivirus deployment, human-related risks including phishing susceptibility, social engineering, credential compromise, and accidental data sharing continued to create persistent attack pathways across the organisational operations between 2021 and 2025.

Conceptual Perspective

IT end-user cybersecurity training is an organizational intervention that ensures all employees, regardless of role or department, receive structured, recurring, and role-relevant instruction designed to reduce the likelihood that human action will result in a security incident. In this study, IT end-user training was hypothesised in terms of training frequency, training modality, role-differentiation, and assessment/certification mechanisms, while human-related cybersecurity risk mitigation was hypothesised in terms of phishing susceptibility (phish rate), risk classification (High/Medium/Low Risk), incident-reporting behaviour (report rate), and employee confidence in identifying threats.

Statement of the Problem

Organisations across the coffee trading and agri-commodity sector in East Africa continue to invest in firewalls, intrusion detection systems, and antivirus infrastructure, yet human-related incidents, phishing, credential compromise, and accidental data disclosure, remain the dominant pathway through which breaches occur. Uganda Coffee LTD experienced this directly in 2021, when a spear-phishing email triggered a ransomware incident despite existing technical defences.

Regardless of the technical safeguards in place, cybersecurity training at Uganda Coffee Ltd has continued to be delivered infrequently, generically, and without role differentiation, formal assessment, or governance accountability. Nearly a third of the workforce (30%) remained untrained or unsure of their training status, and 42.6% had been trained at most once. This has resulted in a persistently elevated phishing risk profile, with 28.7% of employees classified as High Risk. It is upon this basis that this study examined the relationship between IT end-user training and human-related internal cybersecurity risk mitigation, and designed a targeted framework to close the identified gaps.

Objectives of the Study

General Objective

The overall objective of this study was to design and propose a targeted IT End-User Training Framework aimed at mitigating human-related internal cybersecurity risks at Uganda Coffee Ltd.

Specific Objectives

1. To analyse existing IT end-user training frameworks and determine their relevance to organisational operational needs.
2. To evaluate the relationship between IT end-user training and the mitigation of human-related cybersecurity risks.
3. To design a targeted IT end-user training framework tailored to Organizational operational needs to

mitigate identified risks and future threat trends.

4. To evaluate the effectiveness of the designed IT end-user training framework in mitigating internal human-related risks.

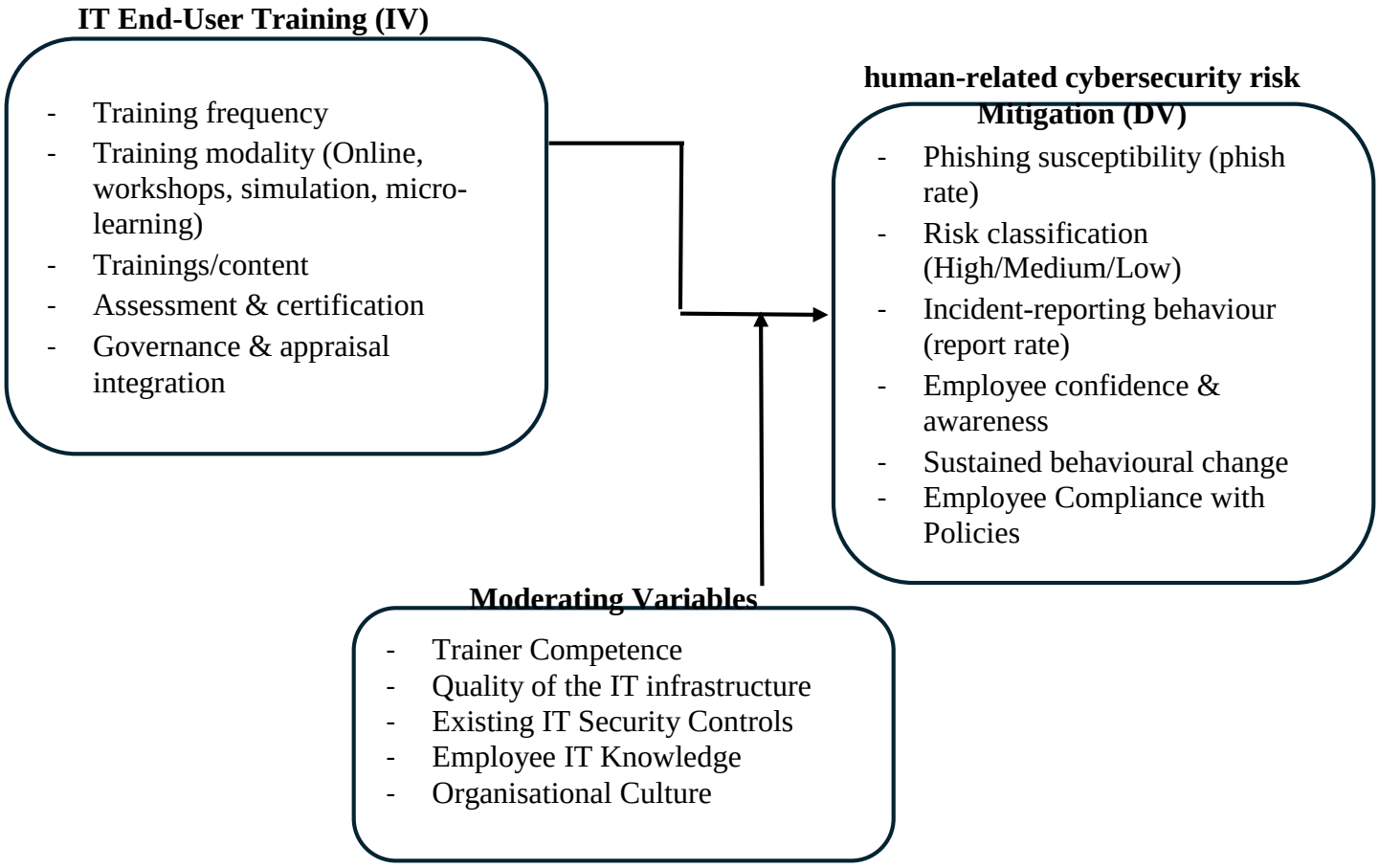
Study Hypothesis

H_0 (Null): Implementing an IT end-user training framework does not lead to a significant reduction in human-related internal cybersecurity risks.

H_1 (Alternative): Implementing an IT end-user training framework does lead to a significant reduction in human-related internal cybersecurity risks.

Conceptual Framework

The conceptual framework displays the linkage between IT end-user training (the independent variable) and human-related cybersecurity risk mitigation (the dependent variable).



Literature Review

IT End-User Training and Human-Related Cybersecurity Risk

The literature consistently identifies human behaviour as the dominant internal cybersecurity risk vector in organisational settings. Verizon's (2024) Data Breach Investigations Report attributes the majority of confirmed breaches to a human element, whether through error, social engineering, or credential misuse. Ncubukezi (2022) argues that human error remains the weakest link for small and medium enterprises specifically because training is treated as a compliance formality rather than a sustained behavioural

intervention. Dash and Ansari (2022) contend that an effective cybersecurity awareness training model functions as the first line of defence in an organisational security strategy, but only when it is delivered with sufficient frequency and contextual relevance to the workforce it targets.

Rogers' (1975) Protection Motivation Theory has been applied extensively to explain why single training events fail to produce lasting behavioural change: threat appraisal and coping appraisal, the two cognitive processes PMT identifies as necessary for protective action, both decay without reinforcement (Sulaiman et al., 2022). This is consistent with Kavärstad's (2022) argument for context-based micro-training delivered in short, frequent cycles rather than annual seminars. Ifinedo (2012) found that policy integration, embedding security behaviour into formal organisational structures such as performance appraisal, is among the strongest predictors of sustained security compliance, a finding that directly informs the appraisal-integration component proposed in this study.

Role differentiation has also emerged as a critical design requirement. Stipesevic, Gunn, and Gunn (2025) found that the perceived relevance of role-based cybersecurity training in the automotive sector was a stronger predictor of engagement than training frequency alone, since employees disengage from generic content that does not reflect their actual operational exposure. Nawaz and Lucas (2024) similarly argue that cybersecurity training for small and medium enterprises must be tailored to address the specific human errors observed within that organisation's own incident history rather than adopting a generic industry template. Ugbebor, Aina, and Kushanu (2024) report that contextualised, role-specific training programmes are associated with a 45 to 65 percent reduction in security incidents, a benchmark this study uses to project the expected effectiveness of the proposed framework.

Assessment and certification mechanisms further reinforce training effectiveness. Koutsouris, Vassilakis, and Kolokotronis (2021) argue that cybersecurity training evaluation metrics are essential to distinguish genuine behavioural change from passive attendance, since training without a measurable outcome cannot be verified as effective. McEvoy and Kowalski (2019) extend this argument through Socio-Technical Systems Theory, holding that technical controls, firewalls, intrusion detection, and antivirus, cannot on their own prevent human-error-induced breaches because they address only the technical dimension of what is fundamentally a socio-technical system; effective interventions must therefore align training, governance, and organisational culture simultaneously.

Methodology

Research Design

This study adopted a quantitative research design, supplemented by a qualitative component drawn from open-ended survey questions. A cross-sectional survey strategy was used, targeting employees during a defined data collection period in early 2026, combined with a case study approach that allowed for an in-depth investigation of cybersecurity training practices within a specific organisational context while generating findings with broader applicability to similar multinational organisations in the East African region.

Study Population and Sample Size

The study population comprised all employees who regularly interact with the organisation's ICT systems, estimated at 280 employees across Operations and Logistics, Finance and Accounting, IT/Technology, Sales and Marketing, Procurement, and other support functions. Using Yamane's (1967) simplified formula ($n = N / (1 + N(e)^2)$) at a 95% confidence level and 5% margin of error, a minimum sample of

165 was indicated. In practice, purposive sampling targeting employees with direct and regular IT-system engagement yielded a final achieved sample of 108 respondents, all of whom completed the survey (100% response rate). In addition, five employees in technical and compliance roles, the HR Manager, IT Security Engineer, Senior Network Engineer, Data and Solutions Engineer, and Compliance Officer, were purposively selected as key informants.

Department / Category	Population	Sample	% of Sample
Operations & Logistics	85	33	30.6%
Finance & Accounting	42	16	14.8%
IT / Technology	18	5	4.6%
Sales & Marketing	20	3	2.8%
Procurement	22	8	7.4%
Other (Field, Support & Admin)	93	43	39.8%
Total	280	108	100%

Table 1: Sample Size Determination and Departmental Distribution (N = 280; n = 108)

Data Collection and Analysis

Primary data were collected through a structured, closed-ended questionnaire designed in Google Forms and distributed electronically to all 108 respondents. Secondary data comprised a phishing dataset covering 1,400 phishing emails from the same 108 employees between 2021 and 2025, obtained from the IT security records. Data were analysed in IBM SPSS using descriptive statistics (frequencies and percentages) for demographic and perception data, and the Chi-Square Test of Independence to examine the association between training status and phishing risk classification, and between gender and training receipt, at a significance level of $p < 0.05$.

Study Findings

Demographic Composition of Respondents

The study gauged the demographic characteristics of the 108 respondents. The results are presented in Table 2.

Category	Items	Frequency	Percentage
Gender	Male	66	61.1%
	Female	42	38.9%
Age Range	18–25 years	4	3.7%
	26–35 years	46	42.6%
	36–45 years	44	40.7%
	46–55 years	13	12.0%

Category	Items	Frequency	Percentage
	56 years and above	1	0.9%
Education Level	Diploma / Certificate	46	42.6%
	Bachelor's Degree	52	48.1%
	Postgraduate (Masters/PhD)	10	9.3%
Job Role	End-User / Staff	76	70.4%
	Supervisor / Team Lead	12	11.1%
	Manager	12	11.1%
	Senior Manager / Director	2	1.9%
	Executive / Managing Partner	3	2.8%
	IT Administrator	3	2.8%

Table 2: Demographic Composition of Respondents (n = 108)

Table 2 shows that the majority of respondents were male (61.1%, n=66), with 83.3% of respondents aged between 26 and 45 years, indicating a predominantly working-age, digitally active workforce. The majority (48.1%) held a Bachelor's Degree, and 70.4% were End-User/Staff, the group representing the primary human-risk layer in organisational cybersecurity and the principal target of the proposed training framework.

Relationship Between Training Status and Phishing Risk Classification

The study examined the relationship between employee training status and phishing outcomes across the five-year dataset (2021–2025, n=108, 1,400 simulations). Table 3 presents the descriptive comparison, and Table 4 presents the Chi-Square test results.

Training Status	n	Avg. Phish Rate (%)	High Risk (n)	High Risk (%)	Report Rate (%)
Trained (Yes)	75	7.3	0	0.0%	30.0
Untrained (No)	24	22.1	22	91.7%	21.8
Unsure	9	15.4	9	100.0%	28.9
Overall	108	11.2	31	28.7%	28.1

Table 3: Phishing Outcomes by Training Status (n=108, 1,400 Simulations, 2021–2025)

Statistic	Value	df	p-value	Interpretation
χ^2 — Full 3×3	99.063	4	< 0.001	Highly significant — reject H_0

Statistic	Value	df	p-value	Interpretation
χ^2 — Trained vs Untrained (2×3)	88.413	2	< 0.001	Highly significant — reject H_0
χ^2 — High vs Not High (2×2)	83.169	1	< 0.001	Highly significant — reject H_0
Cramér's V (3×3)	0.677	—	—	Large effect (V ≥ 0.5)
Phi (φ) (2×2 High/Not High)	0.917	—	—	Very large effect

Table 4: Chi-Square Test Results — Training Status and Phishing Risk Level

The findings in Table 3 and Table 4 showed that there is a very strong, positive, and statistically significant relationship between IT end-user training status and phishing risk classification ($\chi^2(4) = 99.063$, $p < 0.001$), with a large effect size (Cramér's V = 0.677). Trained employees recorded an average phish rate of 7.3% with zero High Risk classifications, compared to 22.1% and 91.7% High Risk among untrained employees, a seven-fold difference in High Risk classification. The study findings suggest that an improvement in the frequency, structure, and role-relevance of IT end-user training strongly and significantly leads to a reduction in human-related cybersecurity risk at Uganda Coffee Ltd. H_0 is rejected; H_1 is supported.

Gender Disparity in Training Receipt

The study further examined whether training receipt was equitably distributed by gender. A statistically significant gender training gap was identified, with male employees receiving training at 78.8% compared to 54.8% for female employees ($\chi^2 = 7.241$, $p = 0.007$), confirming that the training access gap is not attributable to chance and requires deliberate corrective action within the proposed framework's governance structure.

Key Informant Validation

All five purposively selected key informants, the HR Manager, IT Security Engineer, Senior Network Engineer, Data and Solutions Engineer, and Compliance Officer, described real cybersecurity incidents to be attributed to insufficient training, including confirmation of the 2021 ransomware attack's phishing origin. Their recommendations, gathered independently, converged on five distinct structural requirements: a phishing simulation baseline before training design, mandatory quarterly cycles with bi-monthly simulations, role-specific content from inception, a formal certification and records system, and integration of training performance into the annual performance appraisal. None endorsed a voluntary training approach.

The Proposed IT End-User Cybersecurity Training Framework

Building on the empirical findings above, the study designed a five-phase, risk-stratified, role-differentiated IT End-User Cybersecurity Training Framework. The framework is grounded in five theories: Protection Motivation Theory mandates the quarterly training frequency; Human Error Theory mandates the three-tier role stratification; Socio-Technical Systems Theory mandates the governance

layer; Deterrence Theory mandates mandatory participation; and the Behavioural Change Model mandates the certificate and recognition system.

Phase 1: Risk Assessment and Stratification

Before any training is delivered, a phishing simulation baseline is run across all employees to establish individual risk classification: High Risk (phish rate above 20%), Medium Risk (10–20%), or Low Risk (below 10%). Employees are stratified into three operational tiers: Tier 1 (End-Users and Field Staff), Tier 2 (Supervisors and Managers), and Tier 3 (IT Administrators and Executives). High Risk employees receive immediate remedial intervention, priority Module 1 enrolment and monthly simulation, before joining the standard quarterly cycle.

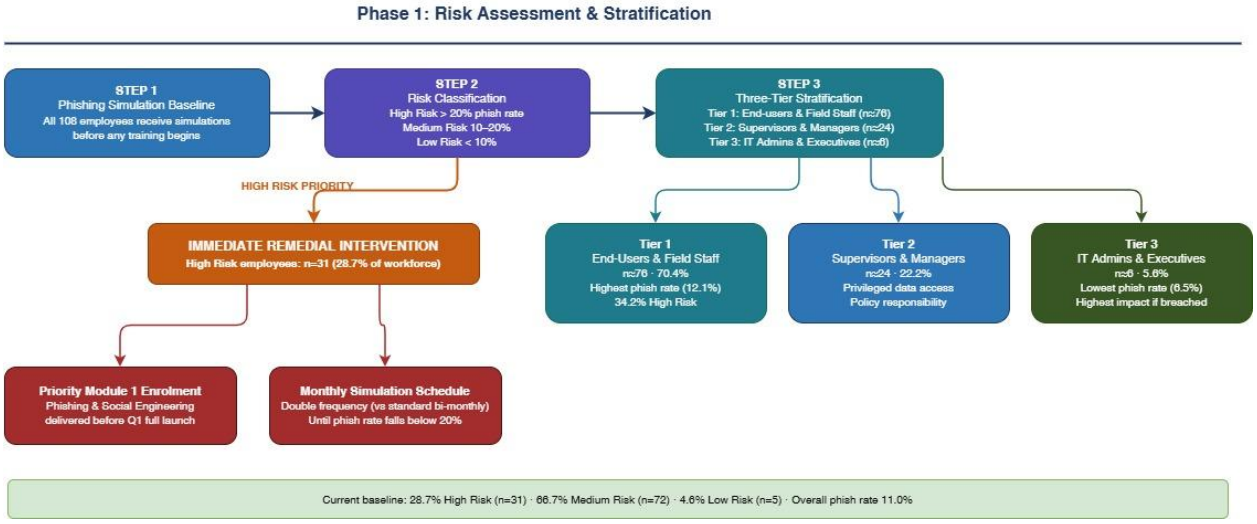


Figure 6.1: Phase 1 — Risk Assessment and Stratification

Phase 2: Mandatory Quarterly Role-Based Training Cycle

Six training modules, phishing and social engineering, password management and MFA, data protection and privacy, safe internet and email use, incident reporting, and role-specific scenarios, are delivered four times per year (Q1–Q4). Every module's content, scenario examples, and assessment questions are adapted to the specific threat exposure of each tier, so that identical learning objectives are taught through entirely role-specific scenarios.

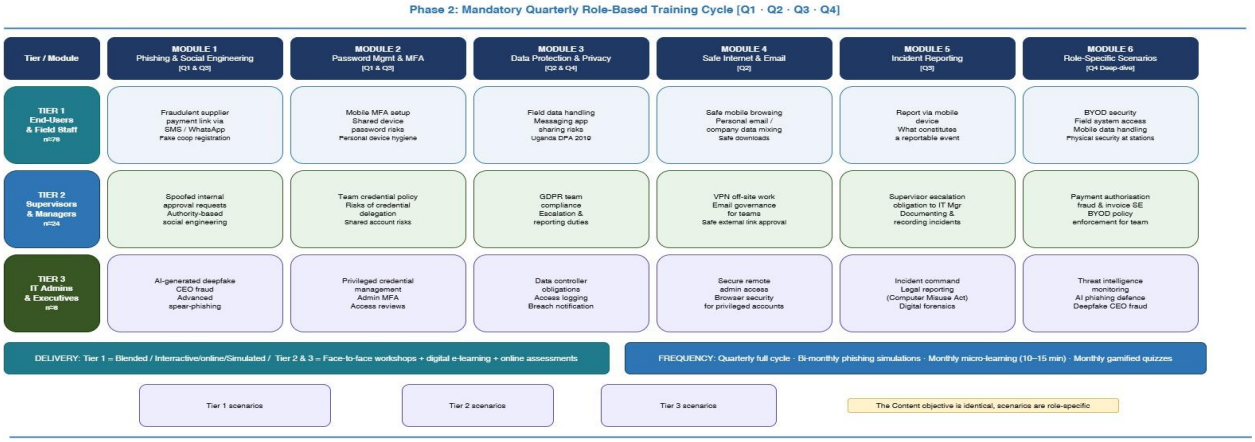


Figure 6.2: Phase 2 — Mandatory Quarterly Role-Based Training Cycle (All six modules differentiated across all three tiers)

Phase 3: Mandatory Assessment and Certification

Each quarterly cycle concludes with a mandatory knowledge assessment requiring a minimum pass rate of 80%. Passing employees receive a digital Certificate of Completion within 24 working hours; employees below the threshold undergo a targeted remedial session and re-sit within two weeks. Employees completing all four quarterly cycles receive an Annual Cybersecurity Compliance Certificate.

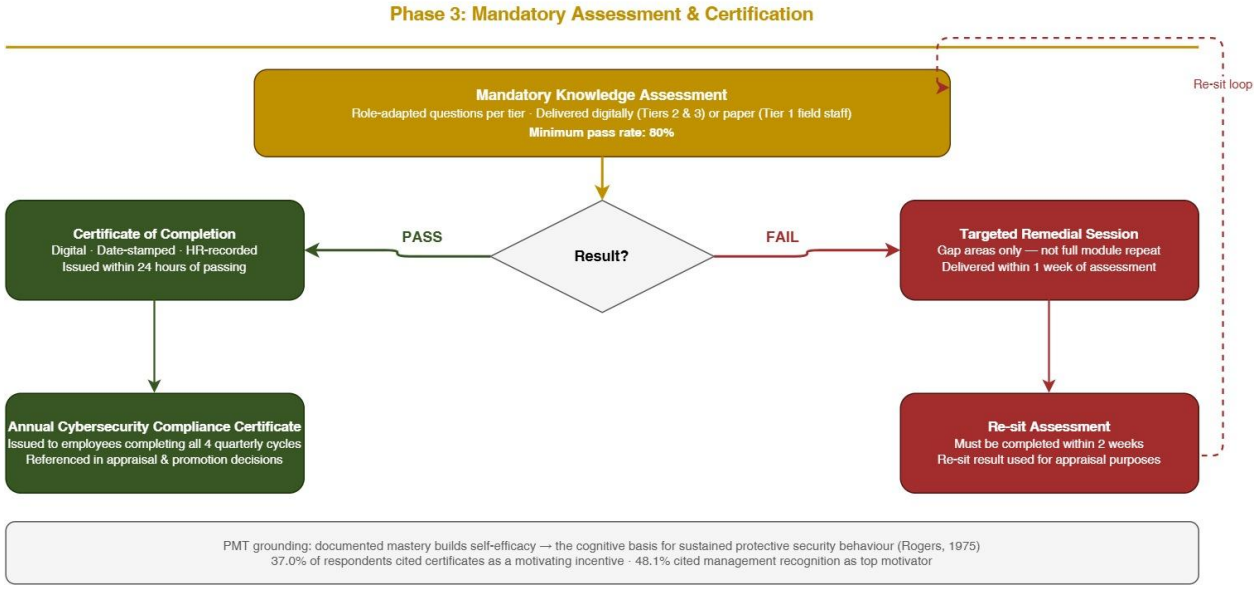


Figure 6.3: Phase 3 — Mandatory Assessment and Certification (Pass/Fail decision gate with remedial loop)

Phase 4: Annual Performance Appraisal Integration

Cybersecurity training performance is formally embedded as a scored criterion in every employee's Annual Performance Appraisal across four weighted sub-dimensions: Quarterly Training Completion (25%), Certificate Attainment (25%), Phishing Simulation Performance (30%), and Incident Reporting Conduct (20%). This transforms training from a discretionary activity into a career-linked professional obligation, consistent with Ifinedo's (2012) finding that policy integration is the strongest predictor of security compliance.

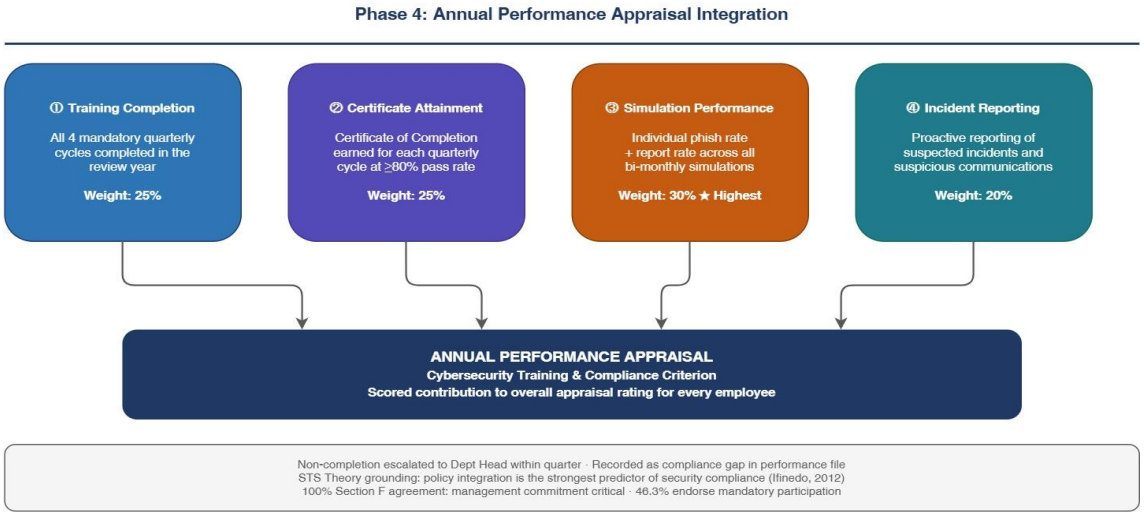


Figure 6.4: Phase 4 — Annual Performance Appraisal Integration (Four scored sub-criteria with weights)

Phase 5: Continuous Evaluation and KPI Review

An adaptive feedback loop tracks eight KPIs quarterly, overall phish rate, High Risk proportion, Low Risk proportion, training coverage, gender training parity, report rate, certificate attainment, and appraisal integration, feeding evaluation outcomes back into Phase 1 for the next cycle.

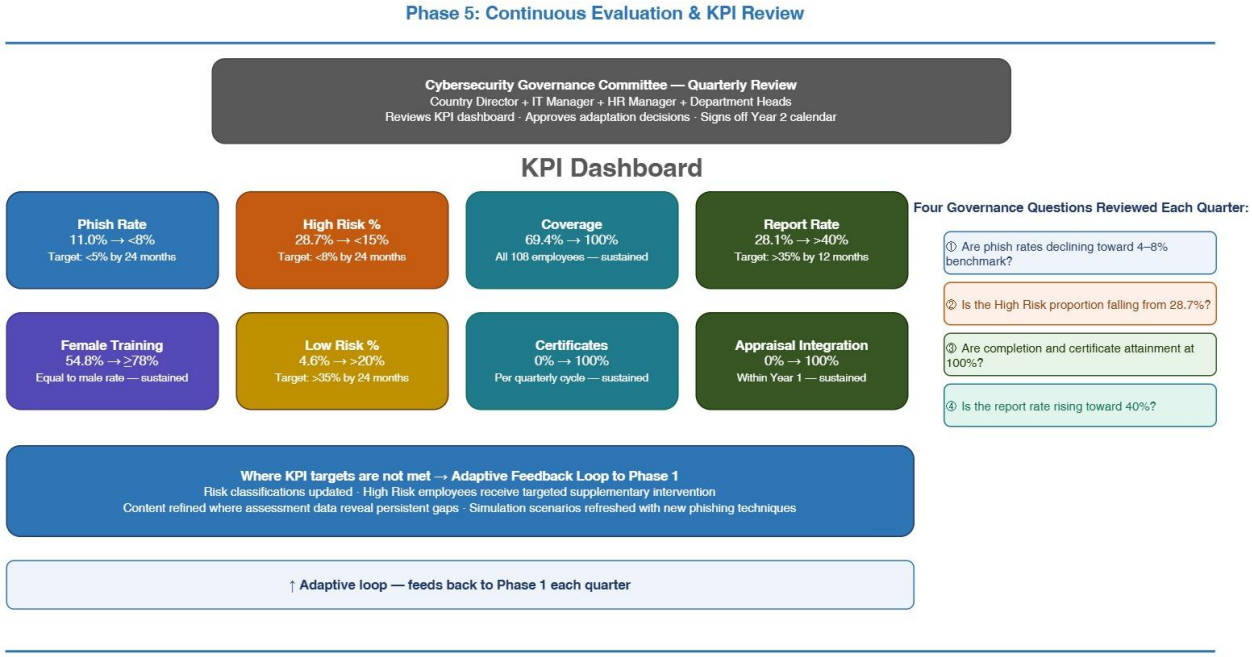


Figure 6.5: Phase 5 — Continuous Evaluation and KPI Review (Eight KPIs with baselines and targets, adaptive feedback loop)

KPI	Current Baseline	12-Month Target	24-Month Target
Overall phish rate	11.0%	< 8.0%	< 5.0%
High Risk employees	28.7% (n=31)	< 15.0%	< 8.0%
Low Risk employees	4.6% (n=5)	> 20.0%	> 35.0%
Training coverage	69.4% (n=75)	100%	Sustained
Female training receipt	54.8%	≥ 78%	Sustained parity
Phishing report rate	28.1%	> 35.0%	> 40.0%

Table 5: Framework KPI Dashboard — Baselines and Targets

The proposed framework was benchmarked against existing models, including NIST CSF 2.0 (NIST, 2024), the SANS Security Awareness framework (SANS Institute, 2024), and commercial platforms such as KnowBe4. None of these reviewed frameworks combine a pre-training simulation baseline, tiered risk stratification, mandatory quarterly delivery, full role-differentiation, formal certification, and appraisal integration in a single model, a combination the proposed framework provides, and which the five key informants independently validated without prior exposure to its design.

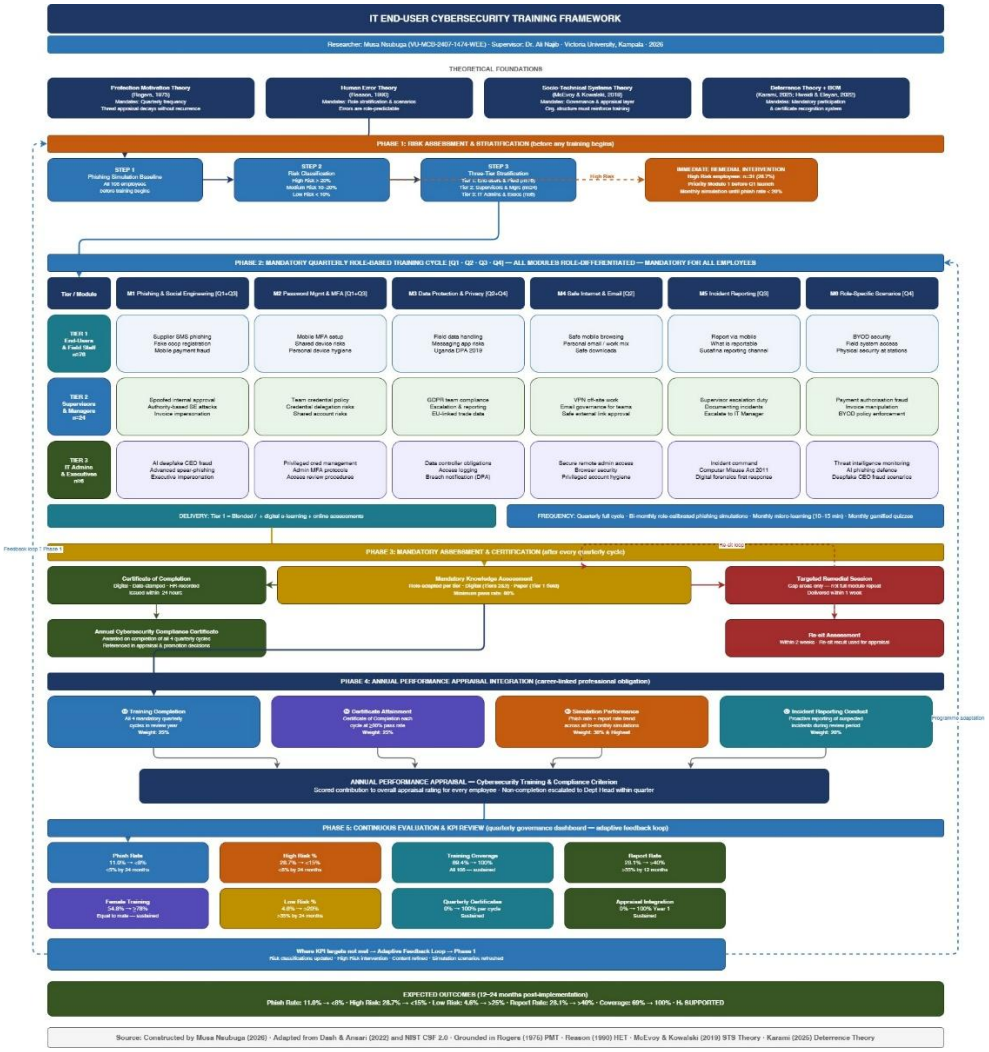


Figure 6.6: The full IT End-User Cybersecurity Training Framework designed using draw.io

Conclusion

The study concludes that IT end-user training, in terms of training frequency, role-differentiation, and assessment/certification mechanisms, is statistically and significantly associated with the mitigation of human-related internal cybersecurity risk, in that an improvement in the structure and delivery of end-user training resultantly leads to a reduction in phishing susceptibility, High Risk classification, and incident frequency. The existing training programme was found to be structurally inadequate: too infrequent, too generic, insufficiently role-relevant, and lacking formal assessment or governance accountability. The phishing dataset provided direct empirical evidence that training is the single most powerful protective variable observed, with trained employees recording a phish rate three times lower and a High Risk classification rate roughly seven times lower than untrained employees, a relationship confirmed as statistically significant ($\chi^2(4) = 99.063$, $p < 0.001$, Cramér's V = 0.677). H_1 is therefore supported.

Recommendations

The study recommends that management should formally adopt the proposed IT end-user training framework as an organisational policy instrument, embedding mandatory quarterly participation within HR policy, IT Acceptable Use Policy, and employment contracts, with non-completion escalated to dep-

artment heads as a recorded compliance gap.

The study also recommends that the IT department implement the five-tier, role-differentiated training curriculum and a structured quarterly phishing simulation programme using scenarios reflective of organizational actual operational communications, while the Human Resources department formally integrates cybersecurity training performance into the Annual Performance Appraisal and issues digital Certificates of Completion to create an auditable, career-linked compliance record.

Finally, the study recommends a longitudinal evaluation of the designed framework's effectiveness following implementation, measuring changes in phishing click-rates, incident frequency, and reporting behaviour over a 12 to 24 month period, and recommends extending this research methodology to other similar operations and comparable East African agri-commodity trading organizations.

References

1. Dash, B., & Ansari, M. (2022). An effective cybersecurity awareness training model: First defense of an organizational security strategy. International Research Journal of Engineering and Technology, 9(7).
2. Hweidi, R., & Eleyan, D. (2022). Social engineering attack concepts, frameworks, and awareness: A systematic literature review. International Journal of Computing and Digital Systems.
3. IBM Security. (2023). Cost of a data breach report 2023. IBM.
4. Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83–95.
5. Karami, A. (2025). Deterrence mechanisms in organisational cybersecurity compliance.
6. Kavärstad, J. (2022). Context-based micro-training: A framework for information security training. Information and Computer Security.
7. Koutsouris, N., Vassilakis, C., & Kolokotronis, N. (2021). Cyber-security training evaluation metrics. Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience.
8. Mai, A., & Khalid, S. (2025). Human reliability analysis in cybersecurity: Applications and implications. Journal of Information Security.
9. McEvoy, G., & Kowalski, S. (2019). Socio-technical integration mechanisms for enhancing cybersecurity system resilience.
10. Nawaz, D., & Lucas, E. (2024). Cybersecurity training for SMEs: Addressing human errors through tailored awareness programs and behavioral risk reduction.
11. Ncubukezi, T. (2022). Human errors: A cybersecurity concern and the weakest link to small businesses.
12. NIST. (2024). NICE cybersecurity workforce framework version 2.0. National Institute of Standards and Technology.
13. Reason, J. (1990). Human error. Cambridge University Press.
14. Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. The Journal of Psychology, 91(1), 93–114.
15. SANS Institute. (2024). Security awareness report 2024. SANS Institute.
16. Stipesevic, J., Gunn, M., & Gunn, I. M. (2025). Exploring factors shaping the perceived relevance of role-based cybersecurity training in the automotive industry.

17. Sulaiman, N., et al. (2022). Evaluating PMT-based cybersecurity training: Improvements in threat appraisal and coping mechanisms.
18. Ugbebor, F., Aina, O., & Kushanu, D. (2024). Employee cybersecurity awareness training programs customized for SME contexts to reduce human-error related security incidents. Journal of Knowledge Learning and Science Technology.
19. Verizon. (2024). 2024 data breach investigations report. Verizon Business.
20. Yamane, T. (1967). Statistics: An introductory analysis (2nd ed.). Harper and Row.