

Original article

Assessing Cybersecurity Awareness among Employees in Libyan Financial Institutions: An Empirical Study

Hesham Almssmari^{*1} , Mustafa Salama¹ , Mansaf Elmansori² 

¹Faculty of Administrative Sciences and Information Technology, UPFA | French Arab University of Africa

³Department of Computer, College of Technical Sciences, Derna, Libya

Email: hso.std82@gmail.com

Abstract

This study assessed cybersecurity awareness among employees in Libyan financial institutions as reliance on digital systems and electronic services continues to grow and exposure to cyber threats increases. Cybersecurity awareness was examined across six dimensions: knowledge of cyber threats, security-policy awareness, authentication and password awareness, phishing and social-engineering awareness, incident-reporting awareness, and secure cybersecurity practices. The study also examined whether cybersecurity training, organizational support, and perceived cyber threat were associated with differences in employee awareness. A quantitative approach was used, based on a structured questionnaire and a five-point Likert scale, with appropriate statistical methods applied to analyze the data and test the proposed relationships and hypotheses. The findings identified areas of strength and weakness in employee awareness. Group comparisons showed a significant difference according to previous cybersecurity training, whereas differences by gender, age, educational qualification, years of experience, and job function were not statistically significant. The results provide a practical basis for developing continuous, role-relevant awareness and training programs, strengthening security policies, and promoting secure practices within Libyan financial institutions.

Keywords. Cybersecurity Awareness, Cybersecurity, Libyan Financial Institutions, Employees, Cybersecurity Training.

Introduction

Financial institutions rely heavily on digital systems to process transactions, manage personal information, authenticate users, and support daily operations. While this reliance offers clear benefits, it also increases exposure to cyber threats. Protecting these systems is therefore not only a technical responsibility; it also depends on management, organizational processes, and the decisions employees make in their daily work [1,2]. Employees are a critical part of this security environment because they work directly with email, applications, authentication systems, customer information, mobile devices, and electronic services. A single decision can strengthen a security measure or weaken it. Recent empirical evidence also shows that human factors remain a major source of security breaches in the financial sector [3,4]. In UAE financial organizations, cyberattack prevention has been linked closely to cybersecurity leadership and employees' day-to-day security behavior [3]. Similarly, a 2025 study of one of Indonesia's largest state-owned banks found that clear security policies and Security Education, Training, and Awareness (SETA) programs significantly improve employee cybersecurity awareness [4]. Current cybersecurity guidance also emphasizes that awareness should be treated as an ongoing process rather than a one-time activity. NIST SP 800-50 Rev. 1, published in 2024, recommends a lifecycle Cybersecurity and Privacy Learning Program that combines awareness campaigns, role-based training, workforce education, measurement, and continuous improvement. The approach recognizes that effective awareness develops over time and needs to remain aligned with changing risks and workplace needs [5].

Recent research has examined employee cybersecurity awareness in developing-country banking, but the evidence remains geographically uneven. Chanda et al. [6] studied 355 bank employees in Bangladesh using PLS-SEM, artificial neural networks, and fsQCA, highlighting the role of employee awareness in protecting against social engineering and other attacks. Al-Kumaim and Alshamsi [3] examined cyberattack prevention in UAE financial organizations, while Akib et al. [4] provided large-scale survey evidence from Indonesian state-owned banks. African evidence is only beginning to accumulate: Hassan et al. [7] reviewed banking cybersecurity practices in Nigeria and concluded that continuous staff awareness programs are among the most practical defenses available to African banks, while Alex-Omiogbemi et al. [8] showed that e-channel fraud in financial institutions is escalating faster than the strategies used to combat it, making employee-facing controls and fraud-awareness training a priority. Together, these studies indicate that awareness is influenced by training, organizational policies, leadership support, and perceived threat, and that empirical evidence is concentrated in South and Southeast Asia and the Gulf states, with much less evidence from North African financial sectors.

Libya illustrates this imbalance clearly. Libyan banks increasingly rely on computerized information systems, electronic payment channels, and online services, while the sector operates in a post-conflict environment marked by fragmented regulation, limited institutional capacity, and uneven investment in security resources. International assessments place African financial sectors among the least cyber-prepared in the world and point to weak supervisory capacity, incomplete incident-reporting systems, and limited awareness and training efforts. Lack of awareness is repeatedly identified as a major obstacle to progress [9].

Against this background, the research gap is specific and definable. First, empirical evidence on cybersecurity awareness among employees in Libyan financial institutions remains scarce; the few locally available assessments are narrow in scope and treat awareness as a limited construct rather than a multidimensional phenomenon covering threat knowledge, security policies, authentication and passwords, phishing and social engineering, incident reporting, and secure daily practices. Second, no prior Libyan study has examined, within a single framework, the roles of cybersecurity training, organizational support, and perceived cyber threat in explaining differences in awareness, nor tested whether awareness of security policies and of phishing actually translates into secure daily practices. Third, existing regional studies in Africa [7,8] have not modeled these organizational and perceptual factors jointly with a separate behavioral outcome. This study addresses all three gaps by providing a comprehensive, multidimensional assessment of cybersecurity awareness among employees in Libyan financial institutions, by jointly testing training, organizational support, and perceived cyber threat as predictors of awareness, and by distinguishing the cognitive dimensions of awareness from the behavioral dimension of secure practices, thereby offering an evidence-based basis for directing training and security efforts.

Rather than viewing cybersecurity as a purely technical issue, this study focused on the employee as a central part of organizational security. It examined awareness of threats, policies, authentication, phishing, incident reporting, and secure practices, while also considering organizational support and perceived threat as associated factors.

Research on information-security awareness has moved beyond a narrow focus on knowledge and increasingly considers the links between awareness, organizational context, and behavior [1,8]. NIST's current guidance describes awareness training as foundational learning that helps personnel understand their role in protecting organizational information, cybersecurity, and privacy assets. The revised SP 800-50 also recommends an ongoing learning-program lifecycle and links awareness with behavior change and security culture [5].

Chanda et al. [6] examined cybersecurity awareness among bank employees in Bangladesh using PLS-SEM, artificial neural networks, and fsQCA. Their results indicated positive relationships involving information-security awareness, knowledge of cyber threats, perceived threat, and perceived vulnerability. This study is particularly relevant because it reinforces the importance of employee cybersecurity awareness within developing-country financial institutions.

Recent research also suggests that employees should not be treated as a homogeneous group. Awareness programs are more effective when they reflect employees' roles, risks, and actual work activities [1,9]. This position is consistent with NIST's role-based learning approach and its emphasis on measuring program effectiveness [5].

At the evidence-synthesis level, Khan et al. [10] conducted a tertiary study of cybersecurity behavioral research, whereas Khan et al. [13] evaluated protection-motivation-based cybersecurity awareness training using Kirkpatrick's model. Accordingly, Reference [10] is used in this study to support broader conclusions from the cybersecurity behavioral literature, while Reference [13] is cited specifically in relation to awareness-training evaluation and behavioral outcomes. Overall, the literature supports viewing cybersecurity awareness through several connected dimensions, including knowledge, policy awareness, threat recognition, secure practices, and training. However, the Libyan financial sector remains underrepresented in this research. This gap provides the main justification for the present study [1,10].

Study Objectives

The study was motivated by two related developments: the growing reliance of financial institutions on digital information systems and the continuing importance of human behavior in cybersecurity. It therefore provides a practical assessment of employee awareness that can help institutions identify weaknesses and determine where awareness efforts should be prioritized. Specifically, the study pursued the following objectives:

Determine the overall level of cybersecurity awareness among employees in selected Libyan financial institutions, identify the strongest and weakest cybersecurity-awareness dimensions, and examine the role of cybersecurity training in employee awareness.

Examine the relationship between organizational support and employee cybersecurity awareness, examine whether perceived cyber threat is associated with higher cybersecurity awareness, and provide practical recommendations for improving cybersecurity awareness programs.

Research Questions and Hypotheses

The study was guided by the following research questions:

RQ1: What is the current level of cybersecurity awareness among employees in selected Libyan financial institutions?

RQ2: Which cybersecurity-awareness dimensions are strongest and weakest?

RQ3: Does cybersecurity training significantly influence employee cybersecurity awareness?

RQ4: Does organizational support significantly influence employee cybersecurity awareness?

RQ5: Does perceived cyber threat significantly influence employee cybersecurity awareness?

Based on these questions, the study tested the following hypotheses:

H1: Cybersecurity training has a significant positive effect on employee cybersecurity awareness.

H2: Organizational support for cybersecurity has a significant positive effect on employee cybersecurity awareness.

H3: Perceived cyber threat has a significant positive effect on employee cybersecurity awareness.

H4: Security-policy awareness has a significant positive relationship with secure cybersecurity practices.

H5: Phishing and social-engineering awareness has a significant positive relationship with secure cybersecurity practices.

H6: Cybersecurity awareness differs significantly according to selected employee demographic and job characteristics.

Theoretical and Conceptual Framework

The study framework assumes that employee cybersecurity awareness is shaped by both individual perceptions and the organizational environment. Training provides knowledge and practical guidance, while organizational support reflects policies, resources, management commitment, and conditions that make it easier for employees to report security incidents. Perceived cyber threat reflects how seriously employees view cyber risks and how relevant those risks seem to their work [1,2].

Cybersecurity awareness was treated as a multidimensional construct, with a clear distinction between awareness—what employees know and recognize—and behavior—what they report doing in practice. Secure Cybersecurity Practices (SP) was therefore defined as the behavioral dimension of the framework: the extent to which employees apply secure procedures in their daily work, including password management, multi-factor authentication, protection of confidential information, and prompt incident reporting. The other dimensions—Security-Policy Awareness (PA), Phishing/Social-Engineering Awareness (PS), Knowledge of Cyber Threats, Authentication and Password Awareness, and Incident-Reporting Awareness—represent the cognitive and knowledge components of awareness. Treating secure practices as a separate behavioral outcome allowed the study to test whether awareness translates into practice (H4 and H5), rather than assuming that knowledge and behavior are the same construct.

The measurement instrument operationalized six constructs: Cybersecurity Training (TR), Organizational Support (OS), Perceived Cyber Threat (PT), Security-Policy Awareness (PA), Phishing/Social-Engineering Awareness (PS), and Secure Cybersecurity Practices (SP). The hypothesized relationships were expressed as follows:

Cybersecurity Training → Employee Cybersecurity Awareness (H1)

Organizational Support → Employee Cybersecurity Awareness (H2)

Perceived Cyber Threat → Employee Cybersecurity Awareness (H3)

Security-Policy Awareness → Secure Cybersecurity Practices (H4)

Phishing/Social-Engineering Awareness → Secure Cybersecurity Practices (H5)

Differences in Cybersecurity Awareness by demographic/job characteristics (H6)

Methodology

Research Design

A quantitative cross-sectional survey design was used to collect standardized responses from employees. The questionnaire provided a structured basis for assessing awareness and examining relationships among the study variables.

Population and Sample

The target population consisted of employees in selected Libyan financial institutions, particularly commercial banks and other financial organizations that rely on computerized information systems and electronic financial services. A total of 120 completed questionnaires were retained for analysis. The sample included employees from information technology, operations, finance, customer service, administration, and management.

Survey Procedure

A structured questionnaire was distributed to employees of the participating institutions during the study's data-collection period. The responses were screened before analysis, and incomplete or invalid questionnaires were excluded. The final dataset contained 120 usable responses.

Measurement Instrument

The questionnaire included items drawn from the relevant literature and organized around six constructs. Responses were recorded on a five-point Likert scale: Strongly Agree (5), Agree (4), Neutral (3), Disagree (2), and Strongly Disagree (1). Compared with the three-point scale used in some earlier reference studies, the five-point scale allowed respondents to express their level of agreement more precisely and was better suited to attitudes and reported security practices. Table 1 summarizes the instrument.

Table 1. Structure of the measurement instrument.

Construct	Code	Items	Main focus
Cybersecurity Training	TR	TR1–TR5	Frequency, relevance, updating, practical exercises
Organizational Support	OS	OS1–OS5	Management, policies, resources, reporting
Perceived Cyber Threat	PT	PT1–PT5	Seriousness, vulnerability, consequences
Security-Policy Awareness	PA	PA1–PA5	Knowledge and application of policies
Phishing/Social Engineering Awareness	PS	PS1–PS5	Threat recognition and verification

Secure Cybersecurity Practices	SP	SP1–SP6	Passwords, MFA, data protection, reporting (behavioral dimension)
--------------------------------	----	---------	--

Validity

Content validity was supported by the relevant literature and reviewed by specialists in cybersecurity, information systems, and research methodology. Before the main survey, a pilot study was conducted to identify unclear or ambiguous items, after which the wording was refined. This process followed recommendations from reviews of cybersecurity-awareness measurement scales, which identify expert review and pilot testing as important steps in instrument validation [12].

Reliability

Cronbach's alpha was used to assess the internal consistency of the questionnaire and its constructs. The coefficients were calculated using the study sample, and the results are presented in Section 7.3.

Data Analysis

The data were analyzed using appropriate statistical software. Frequencies, percentages, means, and standard deviations were used to describe the responses. Cronbach's alpha was used to assess reliability, Pearson correlation to examine relationships among scale scores, and multiple regression to assess the contribution of training, organizational support, and perceived threat to cybersecurity awareness. For H6, Welch independent-samples t-tests were used for two-category variables (gender and previous cybersecurity training), whereas one-way ANOVA (F-tests) was used for variables containing three or more categories (age group, educational qualification, years of experience, and job function). For the five-point scale, scores of 1.00–2.33 indicated low awareness, 2.34–3.67 moderate awareness, and 3.68–5.00 high awareness.

Results**Participants**

A total of 120 completed and usable questionnaires were included in the analysis. The sample comprised 72 men (60.0%) and 48 women (40.0%) and varied in age, educational qualification, professional experience, job function, and previous cybersecurity training. Job functions included information technology, operations, finance, customer service, administration, and management. Fifty-four respondents (45.0%) reported previous cybersecurity training, whereas 66 (55.0%) reported no previous training. These characteristics were examined both to describe the sample and to determine whether awareness differed across the selected employee groups. The complete demographic and job distribution is presented in Table 2.

Table 2. Demographic and job characteristics of the respondents (N = 120).

Variable	Category	n	%
Gender	Male	72	60.0
Gender	Female	48	40.0
Age group	20–29	24	20.0
Age group	30–39	48	40.0
Age group	40–49	32	26.7
Age group	50+	16	13.3
Educational qualification	Bachelor's	72	60.0
Educational qualification	Diploma	18	15.0
Educational qualification	Postgraduate	30	25.0
Years of experience	<5 years	30	25.0
Years of experience	5–10 years	42	35.0
Years of experience	11–15 years	30	25.0
Years of experience	>15 years	18	15.0
Job function	IT	20	16.7
Job function	Operations	28	23.3
Job function	Finance	22	18.3
Job function	Customer service	20	16.7
Job function	Administration	18	15.0
Job function	Management	12	10.0
Previous cybersecurity training	Yes	54	45.0
Previous cybersecurity training	No	66	55.0

Descriptive Results

(Table 3) presents the mean and standard deviation for each study dimension, ranked from highest to lowest. Overall cybersecurity awareness was high ($M = 3.97$, $SD = 0.52$). Perceived cyber threat had the highest mean ($M = 4.21$, $SD = 0.68$), showing that employees clearly recognized the seriousness of cyber risks to their institutions. Phishing and social-engineering awareness ($M = 4.05$, $SD = 0.74$) and security-policy awareness ($M = 3.94$, $SD = 0.79$) were also high. Secure cybersecurity practices scored $M = 3.87$ ($SD = 0.81$), indicating that the behavioral dimension was relatively strong but remained below the main cognitive dimensions. Cybersecurity training ($M = 3.56$, $SD = 0.88$) was moderate, while organizational support had the lowest mean ($M = 3.38$, $SD = 0.91$), also in the moderate range. Overall, the pattern is clear: employees recognized cyber threats and reported relatively strong knowledge and practices, but the organizational conditions that support awareness—particularly systematic training and institutional support—were comparatively weak.

Table 3. Means and standard deviations of the study dimensions ($N = 120$; scale 1–5).

Rank	Dimension	Mean	Std. Deviation	Level
1	Perceived Cyber Threat (PT)	4.21	0.68	High
2	Phishing/Social Engineering Awareness (PS)	4.05	0.74	High
3	Security-Policy Awareness (PA)	3.94	0.79	High
4	Secure Cybersecurity Practices (SP)	3.87	0.81	High
5	Cybersecurity Training (TR)	3.56	0.88	Moderate
6	Organizational Support (OS)	3.38	0.91	Moderate
—	Overall cybersecurity awareness	3.97	0.52	High

Reliability Results

(Table 4) reports Cronbach's alpha values for each construct and for the questionnaire as a whole. All coefficients were above 0.80, indicating high internal consistency.

Table 4. Reliability coefficients ($N = 120$).

Scale / Dimension	Cronbach's Alpha
Overall questionnaire	0.91
Cybersecurity Training (TR)	0.86
Organizational Support (OS)	0.84
Perceived Cyber Threat (PT)	0.88
Security-Policy Awareness (PA)	0.87
Phishing/Social Engineering Awareness (PS)	0.89
Secure Cybersecurity Practices (SP)	0.92

Hypothesis Testing

Pearson correlation and multiple regression analyses were used to examine H1–H5. H6 was examined using group-difference tests selected according to the number of categories in each grouping variable: Welch independent-samples t-tests for gender and previous cybersecurity training, and one-way ANOVA for age group, educational qualification, years of experience, and job function. Table 5 summarizes the hypothesis-testing results.

Table 5. Correlation, regression, and group-difference results ($N = 120$).

Hypothesis/comparison	r	β	Statistic	Sig. (p)	Decision
H1: Training $\rightarrow$ Cybersecurity Awareness	0.58	0.41	$t=5.82$	<0.001	Supported
H2: Organizational Support $\rightarrow$ Cybersecurity Awareness	0.49	0.29	$t=4.17$	<0.001	Supported
H3: Perceived Cyber Threat $\rightarrow$ Cybersecurity Awareness	0.54	0.34	$t=4.96$	<0.001	Supported
H4: Policy Awareness $\rightarrow$ Secure Practices	0.61	0.45	$t=6.31$	<0.001	Supported
H5: Phishing/Social Engineering Awareness $\rightarrow$ Secure Practices	0.56	0.38	$t=5.44$	<0.001	Supported
H6a: Gender (Welch t-test; 2 groups)	—	—	$t=-1.840$	0.069	Not significant
H6b: Age group (one-way ANOVA; 4 groups)	—	—	$F=0.876$	0.456	Not significant
H6c: Educational qualification (one-way ANOVA; 3 groups)	—	—	$F=0.070$	0.932	Not significant
H6d: Years of experience (one-way ANOVA; 4 groups)	—	—	$F=1.519$	0.213	Not significant
H6e: Job function (one-way ANOVA; 6 groups)	—	—	$F=1.922$	0.096	Not significant
H6f: Previous cybersecurity training (Welch t-test; 2 groups)	—	—	$t=2.487$	0.014	Significant

H6 examined whether cybersecurity awareness differed across the selected demographic and job characteristics. No statistically significant differences were found by gender (Welch $t = -1.840$, $p = 0.069$), age group ($F = 0.876$, $p = 0.456$), educational qualification ($F = 0.070$, $p = 0.932$), years of experience ($F = 1.519$, $p = 0.213$), or job function ($F = 1.922$, $p = 0.096$). A statistically significant difference was found only for previous cybersecurity training (Welch $t = 2.487$, $p = 0.014$). H6 was therefore partially supported rather than fully supported. Because H6 concerned group differences rather than regression relationships, no correlation or regression coefficient was reported for these comparisons.

Regression Model

The multiple regression model used cybersecurity training, organizational support, and perceived cyber threat as predictors and produced the following results:

$R = 0.704$

$R^2 = 0.496$

Adjusted $R^2 = 0.478$

$F = 27.84$

Significance < 0.001

The independent variables explained 49.6% of the variance in employee cybersecurity awareness (adjusted $R^2 = 0.478$), and the model was statistically significant at the 0.05 level.

Discussion

Cybersecurity training showed the strongest effect among the three predictors of employee cybersecurity awareness ($\beta = 0.41$, $p < 0.001$), and the model as a whole explained 49.6% of the variance in awareness (adjusted $R^2 = 0.478$). This finding has two layers of meaning. Substantively, it confirms that in a sector where employees handle customer data, payment instructions, and authentication credentials daily, structured exposure to security knowledge is the most efficient organizational investment for raising awareness. Methodologically, the fact that training was the strongest predictor even though its descriptive mean was only moderate ($M = 3.56$) indicates that the participating institutions train inconsistently: employees who received training benefited markedly, but coverage is uneven. This pattern is consistent with Akib et al. [4], who found that SETA programs significantly enhanced cybersecurity awareness among Indonesian state-owned bank employees, and with the continuous, role-based learning model recommended by NIST SP 800-50 Rev. 1 [5]. It also extends the Nigerian review evidence of Hassan et al. [7], who identified continuous staff awareness programs as a practical priority for African banks. The practical conclusion for Libyan institutions is that raising the mean training level, rather than redesigning its content, is the fastest route to raising overall awareness.

Organizational support was positively associated with awareness ($\beta = 0.29$, $p < 0.001$) yet recorded the lowest mean of all dimensions ($M = 3.38$). This combination is informative. The significant coefficient shows that employees who perceive management commitment, clear policies, adequate resources, and workable reporting channels are more aware; the low mean shows that these conditions are not consistently present in Libyan financial institutions. A plausible contextual interpretation is that the post-conflict environment—fragmented regulation, competing institutional priorities, and constrained budgets—has pushed security investment toward visible technical controls and away from the less tangible governance layer of policies, resources, and reporting infrastructure. This mirrors Al-Kumaim and Alshamsi [3], who showed that cybersecurity leadership shapes prevention outcomes in UAE financial organizations, and suggests that in Libya the deficit is not awareness of the need for support but the organizational capacity to deliver it. The relatively modest β for support, compared with training (0.29 vs 0.41), may also indicate that in the absence of systematic programs, employees interpret support signals abstractly, whereas training delivers concrete, usable knowledge.

Perceived cyber threat was the highest-scoring dimension ($M = 4.21$) and a significant predictor of awareness ($\beta = 0.34$, $p < 0.001$). Employees clearly recognize that cyber risks are serious and relevant to their work, and this recognition is associated with higher overall awareness, consistent with Chanda et al. [6], who identified perceived threat and perceived vulnerability as relevant antecedents of cybersecurity awareness among bank employees. However, high perceived threat coexisted with only moderate training and weak organizational support. This pattern can be interpreted in light of the broader cybersecurity behavioral literature synthesized in the tertiary study by Khan et al. [10]: threat recognition alone is unlikely to produce secure behavior unless employees also possess sufficient capability and organizational opportunity. In other words, Libyan employees already possess the motivational raw material; what is missing is the institutional machinery (training, policies, reporting channels) that converts perceived threat into sustained secure practice.

The two strongest relationships in the entire model were security-policy awareness $\rightarrow$ secure practices ($\beta = 0.45$) and phishing/social-engineering awareness $\rightarrow$ secure practices ($\beta = 0.38$), both $p < 0.001$. These results make theoretical and practical sense. Policies translate abstract security goals into concrete, checkable behaviors, so employees who know the policies know what to do; phishing awareness addresses the most frequent attack vector against banks, so employees who recognize social engineering are better positioned to resist it. The findings are consistent with Khan et al. [13], who specifically evaluated protection-motivation-based cybersecurity awareness training using Kirkpatrick's model and reported improvements in training-related behavioral outcomes, and with Alex-Omiogbemi et al. [8], who emphasized that e-channel fraud is best countered by strengthening employee-facing controls. At the same time, the descriptive ranking reveals a knowing-doing gap: the cognitive dimensions (perceived threat 4.21, phishing awareness 4.05, policy

awareness 3.94) all scored above secure practices (3.87). Employees know more than they habitually do. This gap is well documented in the behavioral security literature [10,12] and implies that Libyan institutions should complement awareness content with practice-oriented measures—simulated phishing exercises, rehearsed incident-reporting procedures, and habit-forming routines—rather than relying on instruction alone.

The group-difference analysis provides a more specific picture than the original aggregate H6 statement. Awareness did not differ significantly by gender, age, educational qualification, years of experience, or job function; the job-function comparison approached but did not reach conventional statistical significance ($F = 1.922$, $p = 0.096$). The only significant two-group difference was associated with previous cybersecurity training (Welch $t = 2.487$, $p = 0.014$), indicating that prior training exposure is the group characteristic most clearly associated with awareness in this sample. This finding is consistent with the study's broader emphasis on continuous training and with NIST's role-based learning model [5], while also cautioning against claiming demographic or job-function differences that were not statistically demonstrated.

The findings carry several context-specific implications. First, because training is the strongest lever and currently only moderate, a nationally coordinated, continuous training program—rather than one-off workshops—would yield the largest awareness gains, and its content should reflect the e-channel fraud typologies documented in comparable African markets [7,8]. Second, the organizational-support deficit calls for governance-level action: clear and accessible security policies, visible senior-management commitment, and simple trusted incident-reporting channels. Without these, awareness gains are unlikely to consolidate into behavioral change, as the knowing–doing gap in this study (3.94–4.21 for cognitive dimensions vs 3.87 for practices) already hints. Third, the significant difference by previous training supports expanding and standardizing training coverage. Role-based modules may still be appropriate on risk-management grounds and are consistent with NIST guidance [5], but the present data did not show a statistically significant job-function difference. Fourth, at the sector level, the results provide a baseline that the Central Bank of Libya and individual institutions can use to measure the effectiveness of future awareness initiatives, consistent with the measurement emphasis of the NIST lifecycle approach [5].

Conceptually, the results support treating cybersecurity awareness as a multidimensional construct that is distinct from, though related to, secure behavior [12]. The pattern of significant paths—from training, support, and threat into awareness, and from policy and phishing awareness into practices—fits a staged view in which organizational inputs build awareness, and specific, actionable awareness builds behavior. However, the model left roughly half of the variance in awareness unexplained, indicating that individual factors not measured here—such as self-efficacy, motivation, and security culture—also matter; these should be examined in future Libyan studies. Because the data are cross-sectional and self-reported, the observed relationships should be read as associations rather than confirmed causal effects.

Conclusion

This study assessed cybersecurity awareness among employees in Libyan financial institutions using a multidimensional framework. The questionnaire covered threat knowledge, security policies, authentication, phishing and social engineering, incident reporting, and secure practices, while cybersecurity training, organizational support, and perceived cyber threat were examined as factors associated with differences in awareness. Overall awareness was high ($M = 3.97$). Perceived cyber threat, phishing/social-engineering awareness, security-policy awareness, and secure practices were all in the high range, whereas cybersecurity training and organizational support were moderate and represented the main organizational weaknesses. H1–H5 were supported. H6 was partially supported: awareness differed significantly according to previous cybersecurity training ($p = 0.014$), but no statistically significant differences were found for gender, age, educational qualification, years of experience, or job function. The regression model explained 49.6% of the variance in cybersecurity awareness ($R^2 = 0.496$, adjusted $R^2 = 0.478$, $F = 27.84$, $p < 0.001$).

The main practical value of the study is that it identifies specific areas of weakness rather than treating cybersecurity awareness as a single, general concept. The findings support the development of continuous, role-relevant awareness programs in line with the lifecycle and measurement approach recommended by NIST SP 800-50 Rev. 1 [5]. The multidimensional approach is also consistent with the systematic review of cybersecurity-awareness measurement scales by Rohan et al. [12].

Recommendations

Maintain cybersecurity awareness as a continuous program rather than a one-time activity, consistent with lifecycle-based programs and systematic reviews emphasizing continuous awareness development [1,5].

Provide continuous training that reflects employees' work activities and exposure to cyber risk. The significant difference associated with previous cybersecurity training ($p = 0.014$) supports expanding training coverage, while the non-significant job-function comparison ($p = 0.096$) should be interpreted cautiously.

Use practical phishing and social-engineering examples rather than relying only on theoretical instruction.

Keep cybersecurity policies clear, accessible, and easy to apply in daily work, given the strong effect of policy awareness on secure practices.

Provide simple, trusted channels for reporting suspicious incidents.

Assess awareness periodically and use the results to refine and update training programs.

Ensure that senior management shows visible support for cybersecurity and models secure practices, addressing the organizational-support weakness identified in the descriptive results.

Use the awareness results to set priorities for training and organizational improvements.

Limitations

The cross-sectional design limits causal interpretation of the observed relationships.

The data were self-reported, so responses may be affected by social-desirability bias. In addition, the secure-practices dimension reflects reported rather than directly observed behavior.

Because all constructs were measured with the same questionnaire at the same time, common method bias cannot be ruled out. Future studies should consider procedural remedies, such as separating predictor and criterion measures, as well as statistical diagnostics such as Harman's single-factor test.

The representativeness of the findings depends on the participating financial institutions, and differences among institutions and job roles may affect their generalizability.

The regression model explained 49.6% of the variance in awareness, indicating that other factors not included in the model also contribute to differences in employee awareness.

Future research could use exploratory or confirmatory factor analysis and multicollinearity diagnostics (e.g., VIF) to examine the structure of the measurement model further.

References

1. Khando K, Gao S, Islam SM, Salman A. Enhancing employees' information security awareness in private and public organizations: a systematic literature review. *Comput Secur.* 2022 Jul;118:102749. doi: 10.1016/j.cose.2021.102749.
2. van der Kleij R, Wijn R, Hof T. An application and empirical test of the Capability Opportunity-Motivation-Behaviour model to data leakage prevention in financial organizations. *Comput Secur.* 2020 Oct;97:101970. doi: 10.1016/j.cose.2020.101970.
3. Al-Kumaim NH, Alshamsi SK. Determinants of cyberattack prevention in UAE financial organizations: assessing the mediating role of cybersecurity leadership. *Appl Sci (Basel).* 2023 May 19;13(10):5839. doi: 10.3390/app13105839.
4. Akib AAPM, Candiwan C, Ramadhani DP. Cybersecurity compliance and other factors influencing employee protective behavior: a case study of Bank X in Indonesia. *Int J Saf Secur Eng.* 2025;15(6):1229-1241. doi: 10.18280/ijss.150613.
5. Merritt M, Hansche S, Ellis B, Nethery Snyder J, Sanchez-Cherry K, Walden D. *Building a Cybersecurity and Privacy Learning Program*. Gaithersburg (MD): National Institute of Standards and Technology; 2024. (NIST Special Publication 800-50 Rev. 1). doi: 10.6028/NIST.SP.800-50r1.
6. Chanda RC, Vafaei-Zadeh A, Hanifah H, Nikbin D. Assessing cybersecurity awareness among bank employees: a multi-stage analytical approach using PLS-SEM, ANN, and fsQCA in a developing country context. *Comput Secur.* 2025 Feb;149:104208. doi: 10.1016/j.cose.2024.104208.
7. Hassan AO, Ewuga SK, Abdul AA, Abrahams TO, Oladeinde M, Dawodu SO. Cybersecurity in banking: a global perspective with a focus on Nigerian practices. *Comput Sci IT Res J.* 2024;5(1):41-59. doi: 10.51594/csitrj.v5i1.701.
8. Alex-Omiogbemi AA, Sule AK, Omowole BM, Owoade SJ. Advances in cybersecurity strategies for financial institutions: a focus on combating E-Channel fraud in the Digital era. *Fin Account Res J.* 2024;6(12):2208-2219. doi: 10.51594/farj.v6i12.1771.
9. Barbosa R, Chen B, Khadarina O, Okuda T, Rangachary R, Shao E, et al. Cyber risk: a growing concern for macrofinancial stability. In: International Monetary Fund. *Global Financial Stability Report: The Last Mile, Financial Vulnerabilities and Risks*. Washington (DC): International Monetary Fund; 2024. Chapter 3. doi: 10.5089/9798400257704.082.CH003.
10. Khan NF, Yaqoob A, Khan MS, Ikram N. The cybersecurity behavioral research: a tertiary study. *Comput Secur.* 2022 Sep;120:102826. doi: 10.1016/j.cose.2022.102826.
11. Alshaikh M. Developing cybersecurity culture to influence employee behavior: a practice perspective. *Comput Secur.* 2020 Nov;98:102003. doi: 10.1016/j.cose.2020.102003.
12. Rohan R, Pal D, Hautamäki J, Funilkul S, Chutimaskul W, Thapliyal H. A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon.* 2023 Mar 9;9(3):e14234. doi: 10.1016/j.heliyon.2023.e14234.
13. Khan NF, Ikram N, Murtaza H, Javed M. Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's model. *Comput Secur.* 2023 Feb;125:103049. doi: 10.1016/j.cose.2022.103049.