Guardians Of Banking: Analyzing Cyber Threats İn Turkey's Banking Sector

Dr. Milad Stanikzai †, Doç. Dr. Yusuf Tepeli ††,

†Faculty of Economics and Administrative Sciences, Muğla Sıtkı Koçman University, Muğla, Türkiye
††Faculty of Economics and Administrative Sciences, Muğla Sıtkı Koçman University, Muğla, Türkiye

Abstract
With growing digitalization, the banking sector becomes more vulnerable to cyber-attacks, especially phishing attacks, data breaches, and insider attacks. current study examines cybersecurity awareness among Turkish banking staff following a mixed methods process with a grounding in Protection Motivation Theory (PMT). Quantitative information was gathered from 56 bank employees from 11 banks via Turkish and English language questionnaires, whereas qualitative information was gathered through semi-structured interviews with a senior banker and three university academics of cybersecurity, finance, and digital risk. The findings show broad awareness of cybersecurity, technical, and legal. However, both sets of evidence revealed sophisticated but critical behavioral gaps, first in resisting social engineering, understanding insider threat contexts, and operating in uncertainty. Lastly, the study shows that cybersecurity in banking is not just about technology, it also depends on behavior, organizational culture, and the ability to adapt to new threats.

Keywords:
Cybersecurity Awareness, Turkish Banking Sector, Phishing Attacks, Insider Threats, Data Breaches, Protection Motivation Theory (PMT)

1. Introduction

The world banking sector has experienced explosive digital change over the past two decades, transforming financial services by raising the level of automation, making transactions real-time, and using mobile phones for banking. Yet, all these developments have created a gateway to a new world of high-tech cybersecurity threats. Banks are now prime targets for cybercriminals, not just due to the high value of their electronic money but also due to their growing reliance on complex, interconnected systems (Kshetri, 2021). Among the most threatening risks to banks these days are phishing attacks, data breaches, and insider threats each of which exploits the intersection between technological vulnerabilities and human behavior.

In emerging economies like Turkey, threat vectors are boosted because of asymmetrically enforced rules, irregular organizational readiness, and insufficient sustained spending on cybersecurity building (Eldem, 2021). While Turkish banks have long since entered the future with digital banking innovations, institutions remain dismal on the issue of cybersecurity culture among employees. Arpaci and Ates (2022) argue that the vulnerability of Turkish banks is not only technological but also behavioral in nature since their employees are not properly aware or prepared to identify or respond to cyberattacks. Phishing attacks, in particular, are now more targeted and sophisticated, taking advantage of loopholes in employees' training and security protocols (Zhang et al., 2022).

This study aims to fill an essential research gap in the literature by highlighting employee knowledge specifically of three high-impact cyber threats in Turkish banking: phishing attacks, data breaches, and insider threats. Instead of assessing technological systems or organizational investment plans, this research takes a human approach, examining how front-line employees comprehend, perceive, and react to cyber threats in their everyday jobs. It adopts a mixed-methods strategy, combining quantitative survey answers and expert interviews to provide a multi-dimensional picture of levels of employee awareness and behavioral susceptibility.

Furthermore, the study appeals to Protection Motivation Theory (PMT) to theorize employee behavior in cybersecurity contexts. Initially developed by Rogers (1975), PMT offers a good theory of how individuals assess threats and decide to take protective measures. Applying PMT to the banking sector allows for a deeper understanding of how perceived severity, vulnerability, self-efficacy, and response efficacy influence employees' responses to cyber threats (Ifinedo, 2012). Through the integration of psychological theory and empirical data, the research will provide practical as well as theoretical insights to the discourse in cybersecurity in banking, specifically with regard to such emerging market dynamics as exist in Turkey. İt is worth mentioning that for better understanding, structured and comparative analyses we summarized this literature review in a table format, this

Manuscript received October 5, 2025
Manuscript revised October 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.10.3

review presents the existing knowledge and emphasizes the need for integrated approaches that combine human and technological elements to build a solid cybersecurity framework. (Webster, J., & Watson, R. T. 2002).

2, Literature Review

2.1. Cybersecurity Threats in the Banking Sector

The modern banking sector encounters an evolving cyber threat landscape driven by emerging technologies and sophisticated criminal tactics. Phishing, data breaches, and insider attacks are some of the most prevalent threats, which exploit human errors, poor training, or institutional vulnerabilities (Kshetri, 2021).

Phishing is the foremost cyber threat, especially in Turkey where digital literacy and staff training are limited. Over 90% of the world's cyber intrusions are via phishing (Zhang et al., 2022), occasionally via bank employee targeting through social engineering. Arpaci and Ates (2022) found most Turkish bank employees are unable to recognize or respond to phishing attacks suitably.

Data breaches—attributable to outdated systems, poor authentication, or weak access control—are increasing. The financial sector averages more than $5 million per breach (IBM Security, 2021), making prevention of strategic importance (Arpaci & Sevinc, 2021).

Insider threats, both intentional and unintentional, are the hardest to detect. Long-term employees may use legitimate access to commit fraud (Cummings et al., 2012). Human errors—like weak passwords or clicking on phishing links—also elevate internal threats (Aldawood & Skinner, 2019; Von Solms & Van Niekerk, 2013).

2.2. The Human Factor of Cybersecurity

Human action remains the decider of cybersecurity outcomes. Those organizations that emphasize technology to the exclusion of staff awareness continue to be severely at risk (Alshaikh, 2020). Nowhere is this more true than in banking, where customer-facing staff are often both the first line of defense and the primary targets. Arpaci & Ates's (2022) Cybercrime Awareness Scale (CAS), as validated in Turkish banks, reports that regular training dramatically reduces phishing attacks. On the other hand, banks investing in technology upgrades without complementary human training still report high levels of breaches (Ab Rahman & Choo, 2015). Cybersecurity awareness must be an ongoing process. Technical solutions like encryption and firewalls do not suffice without ongoing education and a strong security culture promoting proactive employee action (Aloul, 2010).

Finally, a general review of international and Turkish studies (Table 1) categorizes current studies into areas like types of threats, employee awareness, technology investment, regulatory loopholes, and ethical standards—enforcing the need to focus on employee-driven awareness in the Turkish banking industry.

Category	Author(s)	Sector/Context	Variables Studied	Methodology	Findings
Cybersecurity Risks	Shehab et al. (2024)	Banking and Financial Services	Malware, data breaches, cyber fraud	Literature Review and Case Analysis	Malware attacks and weak data containment are the most common threats in banking.
	Al-Bassam & Al-Alawi (2020)	Gulf Region	Cyberattack, cybersecurity awareness	Questionnaire and Statistical Analysis	Cybersecurity awareness training improves resilience but requires more funding.
	Karabacak et al. (2016)	Turkish Critical Infrastructure	Regulatory vulnerabilities, attack vectors	Policy Review	Regulatory gaps exacerbate risks, emphasizing the need for a robust legal framework.
	Zwilling et al. (2022)	Global Banking	Human error, digital literacy	Comparative Analysis	Human-targeted cyberattacks like phishing can be decreased through awareness programs.
	Uddin et al. (2020)	Global	Systemic risks, SWIFT hacking	Case Study	Explored vulnerabilities in interconnected financial networks through major incidents.
Employee Awareness	Chanda et al. (2024)	Developing Countries	Awareness training, phishing risk	Multi-Stage Analytical Approach	Employee awareness programs reduce phishing risks significantly in banks.
	Bakhrudin et al. (2023)	Islamic Context	Ethical cybersecurity behavior, Islamic jurisprudence	Survey and Thematic Analysis	Islamic ethics enhance engagement with cybersecurity practices, particularly in data privacy.
	Afzal et al. (2024)	Financial Institutions in India	Cybersecurity awareness, financial inclusion	Analytical Framework	Cyber awareness improves digital inclusion by reducing fraud-related fears.

	Abulhaija et al. (2022)	Jordan Banking Sector	Cybersecurity knowledge, employee behavior	Mixed-Methods Analysis	Positive impact of combining training and technology on security resilience.
Technological Investments	Aloul (2010)	Global Banking	Encryption, firewalls, monitoring systems	Critical Review	Investment in advanced technologies enhances security but is insufficient without staff training.
Regulatory Challenges	Eldem (2021)	Turkish Banks	Regulatory compliance, cybersecurity laws	Policy Analysis	Weak enforcement of regulations increases vulnerability despite existing frameworks.
	(MEPEI, 2023).	MENA Region	Cybersecurity frameworks, policy enforcement	Comparative Analysis	Stricter enforcement and collaboration improve regional cybersecurity.
	Sara Al-Bassam & Adel Ismail (2019)	Bahrain Financial Sector	Governance, board oversight, hacking threats	Online Questionnaire	Highlighted gaps in technical expertise among decision-makers despite prioritizing cybersecurity.
Combined Perspectives	Sugiono, S. (2023).	Global and Islamic Context	Ethical frameworks, technology-human balance	Cross-cultural mixed-methods study (qualitative + quantitative)	Combining Islamic ethical principles with modern cybersecurity practices improves trust, data protection, and long-term security effectiveness

Table 1. *Summary of Key Literature on Cybersecurity Awareness*
Source*: Compiled by the author based on reviewed literature.*

2.3. Research Gaps in the Turkish Context

Despite global progress in cybersecurity, Turkey's banking system remains underexplored empirically. Existing studies often focus on regulatory compliance, technology use, or general awareness, but rarely assess how these elements function within actual bank settings. For instance, Eldem (2021) critiques weak enforcement of cybersecurity laws in Turkey without examining their effects on employee behavior. Likewise, Karabacak et al. (2016) discuss regulatory gaps but overlook how these affect staff training or day-to-day operations.

A core gap is absence of integration of human and technological dimensions. Chanda et al. (2024) urge AI software for fraud detection but note their disablement in the absence of employee understanding and collaboration. Akçakanat et al. (2021) study investments in technology among Turkish banks but do not link them with behavioral readiness. Additionally, cultural and ethical dimensions, such as the place of Islamic ethics on privacy of data, are not usually examined. Komaruddin et al. (2023) argue that ethical theory has the potential to enhance employee engagement in cybersecurity but is still more theoretical in nature and with limited empirical evidence in Turkish banks.

2.4. Conceptual Framework: Protection Motivation Theory (PMT)

To bridge these gaps, the current study adopts Protection Motivation Theory (PMT) by Rogers (1975), which explains how individuals respond to threats through two cognitive processes: threat appraisal (perceived severity and vulnerability) and coping appraisal (response efficacy and self-efficacy). PMT has been a significant model in cybersecurity behavior research (Ifinedo, 2012; Posey et al., 2015).

In banking, PMT helps determine the extent to which employees consider and respond to phishing, data breaches, and insiders. For instance, the employee will be more inclined to follow cybersecurity best practices when they feel they are exposed to threats, view threats as severe, believe that protective measures are effective, and trust themselves to do so. By incorporating PMT, this study extends beyond general awareness to unveil stronger motivations for cybersecurity behaviors, adding psychological depth and placing the work among interdisciplinary academic discourse.

Figure 1 illustrates the four salient PMT constructs—perceived severity, vulnerability, response efficacy, and self-efficacy—mapped to the interview and survey data of the current study. The model provides an explicit theory-to-measurement mapping consistent with prior PMT applications in cybersecurity (Ifinedo, 2012; Mou et al., 2022).

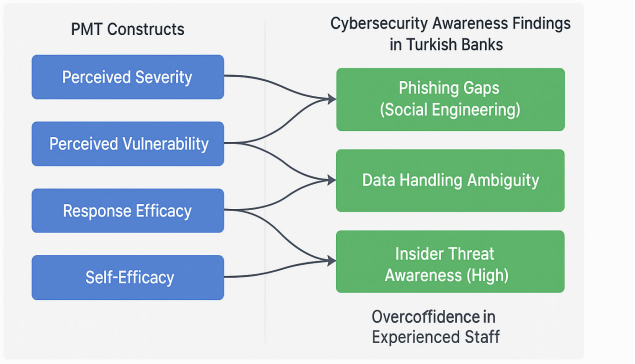

Figure 1. *Conceptual Model: Linking PMT Constructs to Cybersecurity Awareness in Turkish Banking Sector*
Source: *Developed by the researchers based on survey and interview findings.*

3. Methodology

3.1. Research Design

This study employs an exploratory mixed-methods design to examine cybersecurity awareness among Turkish bank employees. Because of both the technical and human nature of cyber attacks, and the paucity of empirical research in this area, this method permits quantification and depth (Creswell & Plano Clark, 2018). Quantitative results quantify prevalence in phishing, data breach, and insider threats, with qualitative expert interview findings bringing richness to context.

A quantitative-only approach would miss behavioral complexity, and a qualitative-only one would be ungeneralizable. Therefore, mixed methods facilitate triangulation to build context-sensitive, evidence-based cybersecurity models.

This model offers both scientific coherence and applied utility—informing Turkish bank policy, training, and security culture, as well as theory development through the use of Protection Motivation Theory (PMT). The research's exploratory character is a precursor to more theoretical models in the future that are based on more thorough, theory-driven approaches.

3.2. Quantitative Data Collection

The survey was completed by 56 respondents from 11 Turkish banks, in various departments and ranks to ensure representative diversity. The survey assessed awareness in four areas:

- General Cyber Threats
- Phishing
- Data Breaches
- Insider Threats

For validity and generalizability, two Turkish-language validated measures were used:

- Cybercrime Awareness Scale (CAS) – assesses recognition and reaction to cybercrime (Arpaci & Ates, 2022).
- Cybersecurity Scale (CS-S) – assesses behavioral practices in cybersecurity scenarios (Arpaci & Sevinc, 2021).

from these 21 items were selected based on their association with:

- Knowledge of cybercrime and ethical internet use
- Methods of identifying phishing
- Data protection responsibilities
- Knowledge of insider threat-inducing behavior

For linguistic and cultural sensitivity, an strict translation process (Brislin, 1970) was followed:

- Expert bilingual forward translation
- Evaluation by a bilingual

- Back-translation to ensure semantic equivalence
- Final verification for contextual and cultural equivalence

This process enhanced the validity and accuracy of the tools for the Turkish banking sector, allowing robust data collection.

3.3. Measurement Scales Overview

Table 2. *overview of Scales Used in the Study*

Variable	Scale Used	Justification
Employee Awareness	Cybercrime Awareness Scale (CAS)	Measures employees' understanding of cyber threats and ability to identify risks.
Phishing, Breaches, Insider Risks	CAS & Cybersecurity Scale (CS-S)	Measures cybersecurity behavior and risk response, aligned with selected threats.

Source: *Compiled by the author based on validated measurement scales.*

As shown in Table 2, both instruments showed high internal consistency. While the Cybercrime Awareness Scale (CAS) showed a Cronbach's Alpha of 0.91, that of the Cybersecurity Scale (CS-S) was 0.88, confirming their reliability and construct validity through both EFA and CFA again (Arpaci & Ates, 2022; Arpaci & Sevinc, 2021).

3.4. Qualitative Data Collection

In order to complement the survey data, semi-structured interviews were conducted with four cybersecurity experts:

- Senior professionals from the banking sector
- University scholars in finance, risk management and cybersecurity threats

The interviews explored:

- Current state of cybersecurity awareness in Turkish banks
- Phishing, data breach, and insider threat issues
- Regulation effectiveness
- The role of employee behavior in security breaches
- Best practices to enhance organizational cybersecurity

Audio recordings of all interviews were transcribed and analyzed thematically following Miles, Huberman, and Saldaña (2020).

3.5. Data Analysis Strategy

A mixed-methods design was employed to gain an overall insight.

Quantitative Analysis (SPSS v26):

- Descriptive statistics (mean, SD, frequency)
- Non-parametric tests (e.g., Mann–Whitney U) to identify subgroup differences by experience or department

Qualitative Analysis (Braun & Clarke, 2006):

Mixed deductive and inductive coding linked to Protection Motivation Theory (PMT) components:

- Perceived severity
- Perceived vulnerability
- Response efficacy
- Self-efficacy

This dual approach enhanced both generalizability and contextual relevance.

3.6. Ethical Considerations

Ethical approval was granted by Muğla Sıtkı Koçman University Ethics Committee (Approval No: 136). Ethical compliance included:

- Informed consent
- Confidentiality of responses
- Voluntary participation
- Permissions from original scale authors (Arpaci, Ates, Sevinc) secured

3.7. Methodological Limitations

Despite its richness, the study was constrained by:

- Small sample size (n = 56) constrains generalizability
- High respondent experience led to low variability, which constrained factor-based statistical testing. These limitations are discussed in detail under Section 8.6.

4. Results

4.1. Quantitative Findings: Cybersecurity Awareness in Turkish Banks

4.1.1. Participant Profile

The survey included 56 employees across 11 banks, across departments:

- Finance (53%)
- IT (13%)
- Other (34%) – e.g., operations, customer service

Notably, 78% had over 6 years of banking experience. Such seniority generated high awareness levels, with minimal variation on most measures, influencing the extent of statistical subgroup analysis.

4.1.2. General Cyberthreats Awareness

This aspect measured internet safety knowledge, legal awareness, and password behavior. It had 7 items (GCSA1–GCSA7) targeted at:

- Knowledge about cybercrime and legal boundaries
- Personal internet safety habits and password hygiene

Table 3. *Descriptive Statistics Summary for GSCA Items*

Item	Mean	Median	Std. Dev.	Min–Max	% Answered "5"
GCSA1	4.86	5.00	0.616	2–5	94.6%
GCSA2	5.00	5.00	0.000	5–5	100.0%
GCSA3	4.96	5.00	0.187	4–5	96.4%
GCSA4	4.55	5.00	0.913	1–5	76.8%
GCSA5	4.98	5.00	0.134	4–5	98.2%
GCSA6	4.84	5.00	0.496	3–5	89.3%
GCSA7	4.68	5.00	0.855	1–5	82.1%

Source: Created by the author based on collected survey data.

The data on table 3 suggest a highly consistent high level of general cybersecurity awareness among the participants:

- GCSA2 achieved a score of 100%, where 100% of the respondents recognized that it is a crime to hack into someone's email account fully exhibiting legal literacy on basic cybercrime.
- GCSA5 (cyberbullying and cyber harassment as a crime) and GCSA3 (use of contact details illegally) followed in exhibiting almost perfect recognition, 98.2% and 96.4% respectively selecting "Strongly Agree.".
- GCSA1, regarding the illegality of use of forbidden programs (i.e., password crackers), and GCSA6, regarding non-disclosure of passwords, both showed excellent compliance, at 94.6% and 89.3% respectively, at the highest level.
- GCSA7, that probed password generation habits (e.g., the inclusion of special characters), showed a bit lower top-level score of 82.1%, showing scope for enhancement in the practice of advanced security.
- GCSA4, facing the need to take legal actions following unauthorized entry into the systems, had the most widespread of responses. Having 76.8% marked "5" and very few scoring only 1 or 2, this question marks different levels of transparency or confidence in policy response mechanisms.

In general, these findings point towards Turkish bank employees possessing high familiarity with key concepts of cybersecurity as well as what is legal. There remains, however, a moderate yet material gap regarding situational or institutional awareness such as escalations of unauthorized access or use of password complexity in practice.

Moreover, these findings align with the professional experience of the sample, the majority of which have a high level of experience, demonstrating that formal training, internal policy, and compliance processes are strong in enforcing general cybersecurity awareness across various roles.

4.1.3. Phishing Awareness

This five-item scale measured employees' behavioral caution and vigilance towards phishing attacks, one of the most widespread and manipulative forms of cyber attacks in banking environments. The five items (PAA1–PAA5) each reflected a different phishing-related behavior such as handling suspect mail, avoiding risky websites, and recognizing social engineering methods.

Table 4. *Descriptive Statistics Summary for PAA items*

Item	Mean	Median	Std. Dev.	Min–Max	% Answered "5"
PAA1	4.80	5.00	0.483	3–5	83.9%
PAA2	4.71	5.00	0.563	3–5	76.8%
PAA3	4.89	5.00	0.366	3–5	91.1%
PAA4	4.50	5.00	0.786	3–5	67.9%
PAA5	4.93	5.00	0.322	3–5	94.6%

Source: Created by the author based on collected survey data.

As we can see in table 4 the findings indicate a very high phishing awareness among the participants:

- PAA5 was the highest compliant, as 94.6% of the participants indicated that they do not open attachments and links from strangers.
- PAA3 and PAA1 also reflected high behavior caution, as 91.1% and 83.9% respectively opted for "Strongly Agree", indicating faith that they are able to identify and avoid typical phishing messages and unknown senders.
- PAA2, warning against sites without security certificates, was slightly lower at 76.8%, possibly due to decreased awareness about

technical indicators like HTTPS among non-IT staff.

- PAA4, social engineering email, had the most variability, with only 67.9% of the participants placing themselves in the top awareness category. This suggests that resistance to psychologically manipulative attacks like tailored scams remains a challenge, even with seasoned personnel.

The findings reflect the effectiveness of Turkish banks' institutional cybersecurity awareness campaigns. However, they also suggest an area where Turkish banks can improve: enhancing employee preparedness against more advanced phishing attacks, particularly those employing social engineering, which have been known to imitate legitimate interaction and require cognitive knowledge as well as training-induced instinct.

4.1.4. Data Breach Awareness

This question assessed employees' perception of data breach threats, namely knowledge about activities involving unauthorized data access, misuse of personal information, and cyber extortion. The five scale items (DBA1–DBA5) captured a specific dimension of breach-related crime and cyber ethics.

Table 5. *Descriptive Statistics Summary for DBA items*

Item	Mean	Median	Std. Dev.	Min–Max	% Answered "5"
DBA1	4.55	5.00	0.829	2–5	73.2%
DBA2	4.52	5.00	0.763	3–5	67.9%
DBA3	4.91	5.00	0.394	3–5	94.6%
DBA4	4.84	5.00	0.626	1–5	91.1%
DBA5	5.00	5.00	0.000	5–5	100.0%

Source: Created by the author based on collected survey data.

In table 5 The results capture high levels of awareness of crime associated with data breaches:

- DBA5 had full agreement, with 100% of those surveyed assuring that cyber extortion via ransomware is a crime a reassuring one considering how ubiquitous and damaging ransomware attacks have become across the globe.
- DBA3 and DBA4, regarding recording without permission and unauthorized access to web sites, showed equally high awareness, with 94.6% and 91.1% respectively selecting "Strongly Agree."
- Consciousness was slightly more varied on DBA1 ("Hacking of information systems is a crime") and DBA2 ("Sharing personal information with third parties is a crime"), with 73.2% and 67.9% respectively choosing the leading response. While still strong, these results could suggest some subtlety about legal boundaries in daily life or organizational contexts particularly in those cultures where information is typically shared between departments or locations.

These results uphold the truth that Turkish bank employees clearly understand what constitutes a data breach and recognize the criminal aspect of primary digital crimes. However, the relatively less confident perspective of procedural or boundary-related scenarios shows the potential for targeted workshops with an emphasis on real-case simulation training programs, especially for data handling, system access, and consent-related media practices.

4.1.5. Insider Threat Awareness

This measure evaluated employees' recognition of threats that come from internal actors either through malicious or careless intent. The items (ITA2–ITA5) covered behaviors such as unauthorized use of login credentials, installation of malware, and sabotage of internal systems significant insider threats in any organizational cyber security model.

Table 6. *Descriptive Statistics Summary for ITA items*

Item	Mean	Median	Std. Dev.	Min–Max	% Answered "5"
ITA2	4.86	5.00	0.483	3–5	91.1%
ITA3	4.95	5.00	0.227	4–5	94.6%
ITA4	5.00	5.00	0.000	5–5	100.0%
ITA5	4.98	5.00	0.134	4–5	98.2%

Source: Created by the author based on collected survey data.

In Table 6 the results reveal an incredibly high level of awareness regarding insider threats:

- TA4 was accepted with full consent, as 100% of the participants accepted that systems corrupting through malicious software (e.g., viruses, Trojans, worms) is a crime.
- ITA5 and ITA3, both concerning cyber blackmail and abuse of social media passwords, reached close with 98.2% and 94.6% of the participants opting for "Strongly Agree."
- ITA2, the one dealing with deliberate disruption or sabotage of computer systems within the organization, also had a bit more variation but otherwise remained very familiar, with 91.1% at the top response level.

These findings indicate not only that workers are cognizant of outside threats but also cognizant of the definition and criminal implications of insider activity a significant aspect of organizational cybersecurity. The high scores may be supported by internal risk management policy, mandatory compliance modules, or firsthand experience with insider security exercises.
Yet, the slight response variation in ITA2 suggests that although insider threats are considered, organizations may still benefit from prioritizing in-house behavior-based security policies, particularly in departments not formally dedicated to IT or network security.

4.1.6. Summary of Cybersecurity Awareness Dimensions Across Key Threat Categories

***Table** 7. Summary of Awareness Levels by Cybersecurity Threat Category*

Category	Items	Mean (Range)	% Answered "5" (Average)	Lowest % "5"	Highest % "5"
General Cyberthreats Awareness	GCSA1–GCSA7	4.84 – 5.00	91.6%	76.8% (GCSA4)	100.0% (GCSA2)
Phishing Attacks Awareness	PAA1–PAA5	4.50 – 4.93	82.9%	67.9% (PAA4)	94.6% (PAA5)
Data Breaches Awareness	DBA1–DBA5	4.52 – 5.00	85.4%	67.9% (DBA2)	100.0% (DBA5)
Insider Threats Awareness	ITA2–ITA5	4.86 – 5.00	96.0%	91.1% (ITA2)	100.0% (ITA4)

***Source:** Developed by the author based on survey response analysis.*

As shown in Table 7, Turkish banking staff indicated very high cybersecurity awareness across all four sections with the majority of items having scores of over 90% on "Strongly Agree" responses.

- Insider Threat Awareness was highest, reflecting good awareness of threats including sabotage, unauthorized access, and malware.
- General Cybersecurity Awareness was high, particularly cybercrime awareness. Escalation procedure awareness (e.g., GCSA4) was lower.
- Phishing Awareness was adequate but less varied. Spam detection was adequate, but awareness of social engineering techniques (PAA4) was weaker, showing a training gap.
- Data Breach Awareness showed good threat identification including unauthorized access and ransomware but weaker awareness of lawful data-sharing procedures, which signifies a need for further policy training.

Overall, staff had strong foundation knowledge, particularly on internal threat and ethical matters, but small areas on subtle human-psychology threats and procedural dealing with data remain.

4.1.7. Non-Parametric Tests

4.1.7.1. Departmental and Experience-Level Comparison

By Department:
Attendees were from:

- Finance (53.6%)
- IT (12.5%)
- Other work (34%)

Main findings:

- IT staff performed best on technical items (e.g., ransomware, malware).
- Finance staff were good on legal/procedural threats but a little poor on phishing and insider threats.
- Other departments were unequally aware, suggesting the need for department-specific training.

All groups had above-average scores in all categories, confirming high institutional awareness, with room for targeted interventions.
By Experience:

- Most of the experienced (6+ years) staff members repeatedly posted high scores, likely due to repeated exposure to training and incidents.
- 1–3 years group showed high awareness, but less consistently on behavioral threats like phishing.
- Smaller subsets (e.g., 3–6 years, <1 year) followed overall trends but were not large enough for in-depth analysis.

4.2. Qualitative Findings

4.2.1. Interview Overview

Four interviews with experts comprised:

- One senior banker
- Three professors at university level in finance, risk managment and cybersecurity

Discussion topics included:

- Current awareness levels
- Major threats: phishing, data breach, insider risk
- Institutional policy and future direction

Interviews were 30–45 minutes long and were audio-recorded, transcribed, and analyzed thematically.

4.2.2. Thematic Analysis

Deductive codes based on PMT (severity, vulnerability, efficacy) and inductive codes derived from interview narratives were used under Braun and Clarke's (2006) six-step approach. This dual approach made labeling employee and institutional behaviors theoretically consistent and empirically dense.

4.2.3. Emergent Themes

Thematic analysis of the four expert interviews three professors at universities and one senior banker found four major themes. These are signs of perceived risks, behavioral facts, and institutional requirements in Turkish banks in the context of cybersecurity. Each theme is translated with Protection Motivation Theory (PMT), emphasizing perceived severity, vulnerability, response efficac y, and self-efficacy.

Theme 1: Perceived Severity of Cyber Threats
All the experts in unison recognized the crucial importance of cyber threats, particularly in the banking area where transactions in the digital realm occur in real-time. The interviewees positioned threats not merely in terms of operations but on individual, institution, and national levels, highlighting the systemic threat posed by even one breach.
"Cybersecurity awareness in Turkey can be evaluated on three dimensions: individual, social, and national… a single employee's error can endanger an entire system." (Interviewee 2)
This theme captures PMT's "perceived severity" construct there is an overall impression by experts that cyber threats are highly risky in that they can lock up digital finance, break public trust, and destabilize institutional systems.

Theme 2: Gaps in Behavioral Vigilance and Overconfidence
While applauding the technological advancement of Turkish banks, experts cautioned against complacency and human mistake as leading causes of insider threats and phishing success. Internal weaknesses, either unintentional or intentional were characterized as more perilous than external assaults.
"Internal vulnerabilities are among the most significant risks to banks. employees unknowingly introducing malware is just as dangerous as an outside hack." (Interviewee 1)
One commentator emphasized the resilience of social engineering in the face of widespread technical controls. This spotlights loopholes in self-efficacy belief that employees can always spot and thwart manipulative strategies. PMT suggests that faith without behavioral readiness degrades an institution's authentic cyber resilience.

Theme 3: Policy Blind Spots and the Need for Cultural Reinforcement
While acknowledging progress in Turkish cybersecurity law (e.g., the 2016 revision of the regulation), the specialists emphasized the need for constant adjustment, pointing to the 2007 Estonian cyber-attack as an international example of institutional readiness.
"Regulations are strong, but cyber threats are evolving faster than policies. Banks need to change from compliance to culture." (Interviewee 4)
This disconnection between formalized form and real-time responsiveness is a mismatch in response efficacy, the premise that existing systems can successfully nullify threats. There was agreement among experts that banks have a tendency to prioritize technical compliance while minimizing the importance of an adaptive security culture.

Theme 4: Future Readiness Through Innovation and Continuous Training
All four of the interviewees emphasized AI, machine learning, blockchain, and autonomous systems as game-changing in countering future threats. Yet technology was not considered enough, it has to be supported by constant employee training, and leadership-innovation.
"Blockchain and autonomous systems will be absolutely key, but without continuous training of employees, they're no more than devices."
"Security needs to be practiced, rather than learned you need simulations, real-case rehearsal, and continued updates."
This most directly speaks to PMT's coping appraisal components: response efficacy (faithfulness in solutions' effectiveness) and self-efficacy (faith in implementing those solutions). Practitioners all agreed that scenario-driven field training and leadership mentoring are the foundation for long-term resilience.

4.3. Integration of Quantitative and Qualitative Results

The convergence of quantitative and qualitative findings revealed a high degree of overall agreement between employee self-reporting awareness and expert assessment of sector-wide readiness. However,

qualitative findings also painted a more detailed yet critical behavioral and structural deficiencies that the survey may not fully disclose. What follows is a thematic difference between important dimensions:

High Awareness Confirmed Across the Dimensions

Survey findings reported extremely high ratings for all four dimensions of awareness: general cybersecurity, phishing, data breaches, and insider threats all items across all categories scored with "Strongly Agree" by over 85% of the respondents. This was echoed in expert opinion, who drew Turkish banking institutions as being generally well-prepared, with staff having a solid foundation knowledge of cyber threats and corresponding legislation.

"The awareness exists especially amongst higher-level personnel. They know what cybercrime looks like, and they've seen its effects." (Interviewee 3)

Convergence: Phishing and Insider Threat Awareness Need Depth, Not Just Breadth

Quantitatively, awareness of phishing was high in general but lower on more low-key items specifically PAA4 ("I ignore social engineering emails"), for which just 67.9% of respondents selected "Strongly Agree." This was echoed vigorously by experts, who pointed out that social engineering may still succeed even in high-awareness environments.

"Knowing something is dangerous doesn't mean people will do the right thing every time especially where manipulation comes into play." (Interviewee 2)

Similarly, insider threat awareness returned the highest average score in the survey (96% agreement), but experts cautioned that such dangers are underestimated due to overconfidence or blindness by the organization.

Divergence: Overconfidence vs Actual Application

Quantitative results hinted at ceiling-level awareness, particularly on the part of senior staff with more than six years' experience. Interviews, however, raised a worry that such may be theoretical or policy awareness instead of behavioral preparedness in the moment.

"It's easy to say you would not click a phishing link in a survey. It's harder to resist when the link seems to be coming from your boss." (Interviewee 1)

This discrepancy reflects a common problem with self-reporting measures: respondents overreport actual skills or answer socially desirable. Qualitative findings refute this by evidencing actual world gaps in behavior, especially in manipulation or when fatigued.

Alignment with PMT: Bridging the Awareness–Action Gap

Across both data sets, Protection Motivation Theory (PMT) provided a coherent interpretive lens:

Table 8. *Alignment of Findings with Protection Motivation Theory (PMT) Constructs*

PMT Construct	Quantitative Evidence	Qualitative Confirmation
Perceived Severity	High agreement across all threats	Experts emphasized sector-level risks and national-scale implications
Perceived Vulnerability	Lower scores on phishing/social engineering	Experts stated staff are often unaware they're vulnerable
Response Efficacy	Strong belief in policies and digital controls	Experts warned policy alone is not enough
Self-Efficacy	Varies strong for laws, weaker for phishing	Experts identified behavioral uncertainty under pressure

Source: Created by the author based on integrated quantitative and qualitative findings.

As observed in Table 8 the convergence between the two data sets supports the reliability of the findings, while the divergence highlights areas where behavioral reinforcement and policy improvement are still needed.

5. Discussion

5.1. Restating the Purpose and Key Findings

This study explored cybersecurity knowledge among Turkish bank staff, namely phishing, data breach, and insider threats—three leading cyber threats to the banking sector. For a mixed-methods PMT-framework study, survey findings (n = 56) from 11 banks were combined with expert interviews. Results revealed consistently high awareness, particularly for legal definitions of cybercrime and password conducts. But there were lapses in behavior in the social engineering scope, implemented policy applied, and threat response achieved. Experts quoted the need for scenario training and complacency and rigid policies as a warning.

5.2 Conclusion Using PMT

Perceived Severity

The topic population closely corresponded with the presence of cyber threats. Legal products (e.g., GCSA2) garnered highest consensus, as would be expected concerning expert concern about institution- and nation-level impacts.

Perceived Vulnerability

Although threat severity was acknowledged, participants low-rated individual vulnerability—particularly in manipulative settings such as social engineering (e.g.,

PAA4). Experts pointed out this discrepancy as a main vulnerability.

Response Efficacy

Participators were guaranteed protection from institutions despite warnings by experts that such a guarantee will be weakened when confronted with new or emergent forms of threats, an indication of exaggerated beliefs in system capability.

Self-Efficacy

Self-efficacy was robust for low-level behaviors (e.g., spam filtering, password protection), but high-level threats eroded this efficacy. As one commentator put it, "It's easy to vow not to click on a malicious link—when it looks like your boss sent it."

The study affirms PMT's worth in explaining cybersecurity behavior but suggests that extensions are required, possibly including deterrence theory (Herath & Rao, 2009) for improved regulation capture in compliance settings.

5.3 Comparison to the Existing Literature

The findings affirm earlier research (e.g., Arpaci & Ates, 2022), and high baseline knowledge regarding Turkish banks. Still, as with Von Solms & Van Niekerk (2013) and Alshaikh (2020), the current study confirms human nature remains the weakest link. It is also in accordance with evidence by Ifinedo (2012) and Posey et al. (2015), where self-efficacy lies behind threat awareness.

In addition, the study adds utility through the application of PMT to a Turkish banking sector, transcending previous survey- or theory-based research. The study adds complexity and specificity to cybersecurity awareness research with the employment of expert triangulation and behavior-based evaluation.

4.4 Practical Implications Key takeaway points for bank managers and cybersecurity administrators

- Awareness ≠ Preparedness: Employees know the risks but don't apply knowledge under pressure or deception. Training should be adaptive, experience-based learning, i.e., simulated phishing and game-based modules.
- Complacency is hazardous: Seasoned employees get overconfident, become lax. Trainings should be tenure- and role-specific, filling departmental blind spots.
- Compliance to culture: Effective cybersecurity requires institutional buy-in, regular refresher training, and inter-departmental coordination—not just policies.
- Tech + Human Synergy: The systems need to be behaviorally resilient and technologically strong, with employee feedback and regular audits.
- Leadership role: Senior management should actively promote continuous improvement by matching cyber intentions with operational realities.

This is in line with Theohari Dou et al. (2005), who argue that even international standards like ISO17799 are futile without cultural and behavioral underpinnings.

5.5 Theoretical Contributions

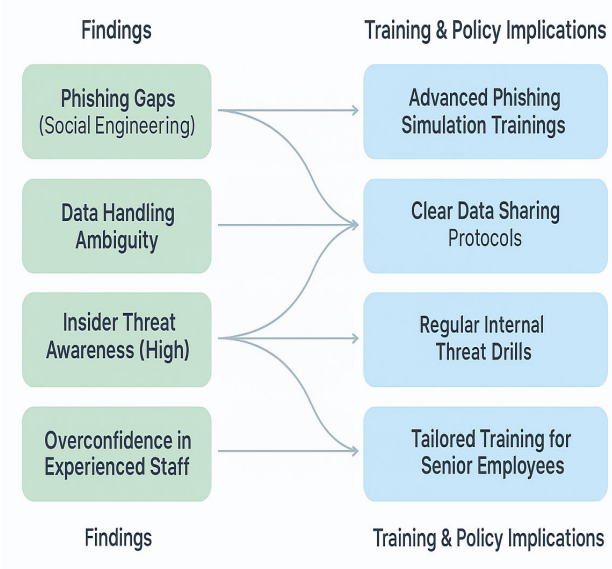

Figure 2. *From Awareness Gaps to Action: Policy and Training Implications Based on Study Findings*
Source: Developed by the researchers based on survey and interview findings.

This study contributes to the novel application of PMT in organizational cybersecurity. It fills a geographic and sectoral field gap in empirical PMT studies by looking at Turkish banks. The mixed-methods approach enhances rigidity, aiming at measurable awareness and situational knowledge. It also condemns PMT's limitations, especially its rationality assumptions of decision. Similar to Mou et al. (2022), this current work recognizes perceived severity and self-efficacy as predictors but not in real, emotion-based attacks. These models must now include organizational culture, emotional, and situation stressors.

In sum, this study confirms the relevance of PMT while advocating for its evolution into a more context-sensitive theory that mirrors human, institutional, and behavioral complexity in cybersecurity.

6. Methodological Limitations

A number of limitations put restrictions on generalizability. One, the limited, experienced sample (n = 56 from 11 banks) can't necessarily be assumed to capture industry dynamics. Ceiling effect is probable as a result of high awareness scores, precluding subgroup comparisons. Two, self-report data provides the opportunity for potential social desirability bias. While interviews provided richness, those too are open to subjectivity.Third, though the measures (CAS and CS-S) were legitimized, low variance in items and sample size excluded more rigorous statistical testing like CFA. Lastly, while PMT provided a sound theoretical framework, it fails to consider completely such elements as leadership, organizational learning, or institution culture.

Despite these limitations, this research provides a helpful benchmarking to the knowledge of cyber security readiness of Turkish banks and leaves the door open for broader, more inclusive studies.

7. Recommendations

Drawing on the collective results of both qualitative and quantitative phases, and theoretical foundation provided by Protection Motivation Theory. (PMT), several recommendations are presented. These are proposed to bridge the gaps in awareness and practice observed, enhance organizational resilience, and promote individual and institutional cybersecurity practices in the Turkish banking industry.

Figure 2 is a visual flowchart that converts principal awareness shortcomings identified in the study into actionable cybersecurity training and policy areas. It distills the empirical findings and cross-references them with Protection Motivation Theory constructs to suggest targeted interventions at the employee and institutional levels. The composite approach is congruent with current literature emphasizing behavior-specific, role-sensitive cybersecurity reinforcement (Posey et al., 2015; Alshaikh, 2020; Mou et al., 2022).

7.1. Behavioral Reinforcement and Employee Training

While levels of awareness were high, via interviews, it was seen that there were strong behavioral gaps—especially in social engineering scenarios. To address this:

- Carry out real-life, bank-specific phishing simulations, including smishing, CEO scams, and deepfake voice scams.
- Use gamified training modules for enhanced participation, especially for front-line staff.
- Offer reminder courses every 6–12 months, refreshed with the most recent threat trends.
- se insider threat monitoring (Shaw et al., 2009) using behavioral audits and peer reporting.
- Align training with PMT constructs:
  - Severity: through real-case simulations
  - Vulnerability: through role-based mapping
  - Response efficacy: through defense success stories
  - Self-efficacy: through scenario-based exercises

5.2. Organizational Policy and Culture Development

Experts stressed that policy must reach beyond compliance into culture:

- Institute a shared sense of responsibility, from senior executives to interns.
- Employ Cybersecurity Champions in every department for localized support.
- Integrate behavioral nudges (e.g., warnings after risky clicks) into systems.
- Make cybersecurity policies not just accessible, but actionable in day-to-day workflow.

5.3. Department-Specific Interventions

Levels of awareness varied across departments:

- Develop role-specific modules:
  - Finance: Data sharing securely, fraud within
  - Operations: Phishing detection, data management
  - IT: Crisis management and advanced threat identification
- Conduct cross-functional simulations to enable collaboration.

5.4. Strengthening Technical and Human Integration

Technology alone is not enough—human behavior needs to be introduced as well:

- Use AI systems that learn from user behavior to offer personalized alerts.
- Look at using blockchain for secure internal transfers.
- Leverage behavior analytics with technical controls to identify insider threats.

- Offer anonymous reporting to shield whistleblowers.

5.5. Leadership and Strategic Alignment

Security needs to be viewed as a board-level concern:

- Offer executive briefings biannually on the threat and response metrics.
- Include cyber risk dashboards in leadership decision-making.
- Designate a CISO who reports to the board or CEO, not just IT.

5.6. Future-Readiness and Continuous Improvement

Forward planning is necessary for ongoing resilience:

- Implement a Cybersecurity Innovation Task Force to track developing threats like quantum threats.
- Collaborate with universities for applied research and audits.
- Publish annual internal Cybersecurity Transparency Reports on threats, reactions, and training.

5.7. Regulator Policy Recommendations

To extend security nationwide:

- Assist benchmarking initiatives by Türkiye Bankalar Birliği or the Central Bank.
- Start certification programs evaluating infrastructure and staff behavior.
- Implement a main cyber incident coordination center to enable real-time bank collaboration.

8. Conclusion

This study sought to explore the extent of employee cybersecurity awareness in Turkish banks, and more specifically, in three high-risk categories: phishing, data breaches, and insider threats. By the combination of quantitative data from 56 bank employees across 11 banks with qualitative insights from four experts, this study provides a rigorous and contextually grounded assessment of human factors shaping cybersecurity readiness in Turkey's banking sector. Research indicated that general awareness levels are remarkably high, especially when it comes to recognizing cybercrime, compliance with password protocols, and the detection of obvious phishing. Nevertheless, both streams of data had one key observation in common: awareness does not always equal readiness at the behavioral level. Specifically, there are gaps in resisting sophisticated social engineering tactics, handling fuzzy data-sharing situations, and managing internal policy weaknesses.

The topic applied Protection Motivation Theory (PMT) to structure and explain these findings, confirming the validity of applying the theory in explaining how the perceived severity of the threat, personal vulnerability, and perceived efficacy influence behavior. At the same time, findings suggest that everyday preparedness and self-efficacy may be more precarious than has been assumed highlighting the need for adaptive, experiential training and cultural facilitation. Apart from theoretical contribution, this study offers tangible practical recommendations to banks, IT managers, regulators, and policymakers. These include scenario-based training, department-level risk education, leadership engagement, and national-level benchmarking processes for sectoral development.

Ultimately, the research determines that banking cyber resilience is more than a technical problem, it is cultural and behavioral. To close the policy-practice gap, and thus the gap between knowing and doing, requires sustained investment in people, process, and responsive strategy. As online threats keep changing, defenses must also improve not just in technology like firewalls and encryption, but also in how employees make decisions and how organizations respond.

References

[1] Afzal, M., Ansari, S., Ahmad, N., Shahid, M., & Shoeb, M. (2024). *Cyberfraud, usage intention, and cybersecurity awareness among e-banking users in India: An integrated model approach*. *Journal of Financial Services Marketing, 29*(3), 1503–1523. https://doi.org/10.1057/s41264-024-00279-3

[2] Al-Alawi, A., & Al-Bassam, S. (2021). *Assessing the factors of cybersecurity awareness in the banking sector*. *Arab Gulf Journal of Scientific Research, 37*(4), 17–32. https://doi.org/10.51758/AGJSR-04-2019-0014

[3] Al-Bassam, S., & Al-Alawi, A. (2019). *Evaluation of telecommunications regulatory practice in the Kingdom of Bahrain: Development and challenges*. *International Journal of Business Information Systems, 31*(3), 282–299. https://doi.org/10.1504/IJBIS.2019.10022047

[4] Aloul, F. A. (2012). The need for effective information security awareness. *Journal of Advances in Information Technology, 3*(3), 176–183.

[5] Alrawhani, E. M., Romli, A., & Al-Sharafi, M. A. (2024). Evaluating the role of protection motivation theory in information security policy compliance: Insights from the banking sector using PLS-SEM approach. *Journal of Open Innovation: Technology, Market, and Complexity, 11*(11), 100463.

[6] Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98*, 102003.

[7] Arpaci, I., & Ates, Y. (2022). Cybercrime awareness among university students: Evidence from Turkey. *Security Journal, 35*(1), 1–15.

[8] Arpaci, I., & Sevinc, H. (2021). Investigating the role of personality traits and cyber security awareness on mobile phone users' security behavior. *Computers in Human Behavior Reports, 3*, 100068.

[9] Bakhrudin, B., Margolang, F., Sudarmanto, E., & Sugiono, S. (2023). *Islamic perspectives on cybersecurity and data privacy: Legal and ethical implications*. *West Science Law and Human Rights, 1*(4), 166–172. https://doi.org/10.58812/wslhr.v1i04.323

[10] Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do users have to fear? Using fear appeals to

engender threats and fear that motivate protective behaviors in users. *MIS Quarterly, 39*(4), 837–864.
[11] Cummings, A., Lewellen, T., McIntire, D., Moore, A., & Trzeciak, R. (2012). Insider threat study: Illicit cyber activity involving fraud in the U.S. financial services sector. *Software Engineering Institute, Carnegie Mellon University.*
[12] Eldem, T. (2019). The Governance of Turkey's Cyberspace: Between Cyber Security and Information Security. *International Journal of Public Administration*, *43*(5), 452–465. https://doi.org/10.1080/01900692.2019.1680689
[13] Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology, 30*(2), 407–429.
[14] Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems, 18*(2), 106–125.
[15] 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.
[16] Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549–566.
[17] Karabacak, B., Yildirim, S. O., & Baykal, N. (2016). A vulnerability-driven cyber security capability maturity model for measuring national cyber security capability. *International Journal of Information Security Science, 5*(2), 1–14.
[18] Lee, D., Larose, R., & Rifon, N. J. (2008). Keeping our network safe: A model of online protection behavior. *Behaviour & Information Technology, 27*(5), 445–454.
[19] MEPEI. (2023, October 6). *Cybersecurity strategies of MENA countries*. Middle East Political and Economic Institute. https://mepei.com/cybersecurity-strategies-of-mena-countries/
[20] Mkilia, E., Kaleshu, J. T., & Sife, A. S. (2023). Cybersecurity risks and customers' protective behavior on usage of mobile banking services: Evidence from selected banks in Tanzania. *COLAKKU Journals, 5*(2), 23–35.
[21] Mou, J., Cohen, J. F., Bhattacherjee, A., & Kim, J. (2022). A test of protection motivation theory in the information security literature: A meta-analytic structural equation modeling approach. *Journal of the Association for Information Systems, 23*(1), 196–236.
[22] Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems, 32*(4), 179–214.
[23] Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91*(1), 93–114.
[24] S. Abulhaija, S. Hattab and A. Qusef, "Cyber Security Awareness, Knowledge and Behavior in the Banking Sector in Jordan," *2022 13th International Conference on Information and Communication Systems (ICICS)*, Irbid, Jordan, 2022, pp. 48-53, doi: 10.1109/ICICS55353.2022.9811212.
[25] Shaw, E., Fischer, L., & Rose, A. (2009). Insider risk evaluation and audit. *Department of Defense Personnel Security Research Center.*
[26] Shehab, R., Abrar, S., Almaiah, M., Alkhdour, T., Belal, M., Alwadi, B., & Alrawad, M. (2024). *Assessment of cybersecurity risks and threats on banking and financial services*. *Journal of Internet Services and Information Security, 14*(3), 167–190. https://doi.org/10.58346/JISIS.2024.I3.010
[27] Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity behavior among government employees: The role of protection motivation theory and responsibility in mitigating cyberattacks. *Information, 13*(9), 413.
[28] Tambariki, C., Sondakh, O. B., Dondokambey, V. A., & Hendriana, E. (2024). Drivers of banking consumers' cybersecurity behavior: Applying the extended protection motivation theory. *Global Academy of Training and Research Journal, 9*(1), 1–15.
[29] Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security, 24*(6), 472–484.
[30] Uddin, M., Hakim, B. M., & Hassan, M. K. (2020). *Cybersecurity hazards and financial system vulnerability: A synthesis of literature*. *Risk Management, 22*(4), [no page numbers provided]. https://doi.org/10.1057/s41283-020-00063-2
[31] Utama, A. S., Sudarmanto, E., & Sugiono, S. (2023). Islamic perspectives on cybersecurity and data privacy: Legal and ethical implications. *West Science Law and Human Rights*, *1*(4), 166–172. https://doi.org/10.58812/wslhr.v1i04.323

Doç. Dr. Yusuf Tepeli is an Assistant Professor in the Department of Accounting and Finance at Muğla Sıtkı Koçman University in Turkey. His major research interests include financial performance analysis, corporate finance, accounting education, and sustainable finance. He has published extensively in national and international journals and serves as an editor for the *Journal of Entrepreneurship, Innovation, and Marketing Research*.

Milad Stanikzai is a PhD candidate in the Department of Finance at Muğla Sıtkı Koçman University, Turkey. He holds an MA in Finance and Banking from Kabul University, Afghanistan, and a BBA in Business Administration from Parwan University. His research focuses on financial risk management, cybersecurity in banking, sustainable finance, and the socioeconomic impacts of scholarship programs. With professional experience spanning academia, banking, and public sector finance including roles at Albironi University, Azizi Bank, and the Afghan Ministry of Defense he brings expertise in financial analysis, policy training, and cross-cultural communication. Fluent in English, Turkish, Persian, and Pashto, he is actively working on research projects targeting high-impact journals in finance, public health, and education policy.