Pakistan Journal of Management Sciences and Technology (PJMST)
http://www.pjmst.com/index.php/ojs
Volume 3, Issue 3 (2025)

DIGITAL SECURITY AWARENESS AND BEHAVIORAL INTENT TO ADOPT DIGITAL SAFETY PRACTICES AMONG TELECOM SECTOR EMPLOYEES IN PAKISTAN

Dr. Ayesha Rafi
National University of Sciences & Technology (NUST), Islamabad, Pakistan
Email: ayesha.rafi.research@gmail.com

Abstract

As telecom firms in Pakistan expand digital operations, employee behavior has become a frontline defense against cyber threats. This quantitative study examines how cybersecurity awareness, perceived organizational support, perceived severity of cyber threats, and self-efficacy predict employees' behavioral intention to adopt digital safety practices. A structured survey was administered to 520 employees across three major telecom operators and regional offices. Using reliability analysis, confirmatory factor analysis (CFA), and structural equation modeling (SEM), results indicate that cybersecurity awareness, perceived organizational support, and self-efficacy significantly and positively predict behavioral intention, while perceived severity has an indirect effect mediated by self-efficacy. Practical implications include targeted training design, leadership engagement, and integrating behavioral nudges into daily workflows. The study contributes empirically to organizational cyber-behavior literature in emerging markets and offers actionable recommendations for telecom HR and security teams.

Keywords: *Cybersecurity Awareness, Behavioral Intention, Perceived Organizational Support, Self-Efficacy, Telecom, Pakistan*

Introduction

Cyber threats have become persistent and sophisticated, and employees are often the most exposed actors in organizational security chains. For telecom companies providers of critical communication infrastructure and processors of massive customer data employee adherence to basic digital safety practices (strong passwords, two-factor authentication, phishing vigilance, secure file sharing) is essential to prevent breaches that can cascade into national-level disruptions and reputational damage. Pakistan's telecom sector has grown rapidly, but with growth comes exposure: a mobile-first population, expansive customer databases, and increasing digitization of processes create attractive targets for attackers.

Research shows that technical controls alone are insufficient; human behavior is a decisive factor in cybersecurity outcomes (Ifinedo, 2012; Parsons et al., 2017). Employee knowledge (cybersecurity awareness), the organizational environment (perceived organizational support for security), individuals' beliefs about threat seriousness (perceived severity), and confidence in their capacity to perform safe behaviors (self-efficacy) jointly influence whether employees intend to adopt and actually perform safe practices (Bandura, 1997; Ajzen, 1991).

This study aims to quantify these relationships in Pakistan's telecom context. The research addresses four primary questions:

1. To what extent does cybersecurity awareness predict employees' behavioral intention to adopt digital safety practices?
2. How does perceived organizational support (POS) for cybersecurity influence behavioral intention?
3. What role do perceived severity and self-efficacy play in shaping intentions?
4. Are the effects robust after controlling for demographic factors (role, tenure, digital literacy)?

By focusing on telecom employees, this paper provides sector-specific evidence to guide employee-facing interventions and contributes to the limited empirical literature on cyber-behavior in South Asian organizations.

Literature Review

Cybersecurity Awareness and Employee Behavior

Cybersecurity awareness refers to knowledge about cyber risks, indicators of phishing, appropriate password hygiene, and safe online practices (Puhakainen & Siponen, 2010). Studies consistently find awareness to be a primary predictor of security-compliant behavior (Bulgurcu, Cavusoglu, & Benbasat, 2010). In organizational contexts, awareness campaigns increase detection of suspicious emails, reduce risky clicks, and improve reporting rates (Hadlington, 2017). However, awareness without practical reinforcement (procedures, feedback, tools) often yields limited behavioral change (Johnston & Warkentin, 2010).

Perceived Organizational Support and Security Culture

Perceived organizational support (POS) employees' belief that their organization values their contributions and cares for their well-being extends to security: when employees perceive that management prioritizes cybersecurity through resources, training, and leadership messaging, they are more likely to comply with security policies (Eisenberger et al., 1986; Ifinedo, 2012). POS can create a security climate that normalizes protective behaviors and reduces perceptions that security is an optional burden rather than an integral work component.

Perceived Severity and Protection Motivation

Protection Motivation Theory (PMT) posits that perceived severity (how serious one believes consequences of a threat are) and perceived vulnerability motivate protective behaviors (Rogers, 1975). Perceived severity alone may not guarantee action; it often operates via cognitive appraisals of coping efficacy (e.g., self-efficacy) and response efficacy (belief that the recommended action will mitigate risk). In workplace cyber contexts, employees who perceive severe consequences for breaches are more attentive, but only if they believe they can take effective measures (Boss et al., 2009).

Self-Efficacy and Behavioral Intention

Self-efficacy confidence in one's ability to execute specific behaviors (Bandura, 1997) — correlates with stronger intention and performance. In cybersecurity studies, self-efficacy predicts the consistent use of security tools (e.g., configuring 2FA), correct handling of suspicious messages, and adherence to protocol (Chen & Zahedi, 2016).

Integrated Models and Telecom Sector Relevance

Integrating awareness, POS, perceived severity, and self-efficacy aligns with socio-cognitive and organizational behavior frameworks. Telecom firms, given their scale and customer-facing responsibilities, require employees to be both aware and empowered. Empirical studies from developed contexts suggest these variables explain a sizable portion of variance in security behavioral intentions (Ifinedo, 2012; Parsons et al., 2017), but there is limited sector-specific evidence in emerging markets like Pakistan. This study fills that gap.

Hypotheses

Derived from the literature, the model proposes direct and mediated relationships:

H1: Cybersecurity awareness positively predicts behavioral intention to adopt digital safety practices.

H2: Perceived organizational support (POS) positively predicts behavioral intention.

H3: Perceived severity is positively associated with behavioral intention.
H4: Self-efficacy positively predicts behavioral intention.
H5: Self-efficacy mediates the relationship between perceived severity and behavioral intention.
H6: The primary effects (H1–H4) remain significant after controlling for role (technical vs. non-technical), tenure, and self-reported digital literacy.

Methodology

Research Design and Sample

A cross-sectional quantitative survey design was used. Data were collected in 2025 from employees of three major telecom operators and associated regional offices in Pakistan (Karachi, Lahore, Islamabad, Peshawar). The sample comprised 520 employees (response rate ~65% from 800 distributed surveys). Participants included technical staff (network engineers, security operations; 46%), customer-care and operations staff (30%), and managerial/administrative personnel (24%). Tenure ranged from under 1 year to 20+ years (mean = 6.3 years). Digital literacy was self-assessed (1–5 scale; mean = 4.1).

Instrument Development

The questionnaire combined validated scales adapted to context:

- **Cybersecurity Awareness (AW)**: 8 items adapted from Puha Kainen & Siponen (2010) and Ifinedo (2012) (e.g., "I can identify the signs of a phishing email").
- **Perceived Organizational Support for Security (POS)**: 6 items adapted from Eisenberger et al. (1986) and security-climate literature (e.g., "Management provides adequate security training and resources").
- **Perceived Severity (PS)**: 4 items adapted from PMT literature (e.g., "A security breach could have serious consequences for our customers and the company").
- **Self-Efficacy (SE)**: 6 items measuring confidence to perform protective actions (e.g., "I am confident I can securely configure my work devices").
- **Behavioral Intention (BI)**: 5 items measuring intent to perform or sustain security behaviors (e.g., "I intend to follow security procedures consistently").

All items used a 5-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree). The instrument was pilot-tested with 40 employees from a regional office; wording was adjusted for clarity.

Data Collection Procedure

After IRB approval from NUST, HR/security teams at participating firms circulated the survey link and paper forms where needed. Participation was voluntary; anonymity was assured. Data collection occurred over six weeks. Completed surveys were checked for missing data; incomplete responses (>20% missing) were discarded, leaving 520 usable cases.

Data Analysis

Analyses proceeded in steps:

1. Descriptive statistics and demographic profiling.
2. Reliability analysis (Cronbach's alpha) and CFA (AMOS v27) to confirm factor structure and construct validity. Fit indices examined: CFI, TLI, RMSEA, SRMR.
3. Structural Equation Modeling (SEM) to test hypothesized paths; bootstrapping (5,000 samples) used to test mediation (Hayes-style).
4. Multi-group/regression controls to assess robustness across roles, tenure, and digital literacy.

Results

Descriptive Statistics and Reliability

Interpretation: Prior to testing the structural model, internal consistency and descriptive patterns help understand baseline readiness. Means show generally positive scores, with awareness and self-efficacy relatively high, POS moderate, and perceived severity elevated — indicating employees recognize threat seriousness.

Table 1. Descriptive Statistics and Reliability (N = 520)

Construct	Items	Mean (SD)	Cronbach's α
Awareness (AW)	8	4.21 (0.56)	0.88
Perceived Organizational Support (POS)	6	3.74 (0.72)	0.86
Perceived Severity (PS)	4	4.12 (0.65)	0.83
Self-Efficacy (SE)	6	4.05 (0.61)	0.87
Behavioral Intention (BI)	5	4.09 (0.59)	0.89

All Cronbach's α values exceed 0.80, indicating strong internal consistency across scales

Confirmatory Factor Analysis

Interpretation: CFA examined whether items loaded on intended latent constructs. Model fit indices indicate acceptable fit: CFI = 0.96, TLI = 0.95, RMSEA = 0.038 (90% CI: 0.034–0.042), SRMR = 0.039. All standardized factor loadings ranged from 0.62 to 0.88 ($p < .001$), supporting convergent validity.

Correlations

Interpretation: Correlation analysis indicates expected positive associations among predictors and with behavioral intention, suggesting the conceptual model is viable.

Table 2. Zero-order Pearson Correlations (N = 520)

Variable	1	2	3	4	5
1. AW	1				
2. POS	.44**	1			
3. PS	.39**	.36**	1		
4. SE	.48**	.40**	.51**	1	
5. BI	.56**	.49**	.45**	.59**	1

Note: **p < .01

Structural Model Results

Interpretation: SEM tested H1–H5 simultaneously. Paths from AW, POS, and SE to BI are significant and positive. PS did not have a strong direct path to BI once SE was included; mediation analysis suggests its effect operates largely through SE.

Table 3. SEM Path Coefficients

Path	Standardized β	SE	t-value	p-value
AW → BI	0.30	0.04	7.50	< .001
POS → BI	0.21	0.03	6.00	< .001
SE → BI	0.34	0.04	8.50	< .001
PS → BI	0.06	0.03	1.80	.071
PS → SE	0.48	0.04	12.00	< .001

Model explains 62% of variance in Behavioral Intention ($R^2 = 0.62$). Fit indices: CFI = 0.95, TLI = 0.94, RMSEA = 0.041, SRMR = 0.045.

Mediation Analysis

Interpretation: Bootstrapped indirect effects show PS → SE → BI is significant: indirect effect = 0.16 (95% CI: 0.12–0.20), $p < .001$, supporting H5 that self-efficacy mediates perceived severity's impact on intention.

Controls and Robustness

Interpretation: Including role (technical vs. non-technical), tenure, and digital literacy as covariates did not substantially change the magnitude or significance of primary predictors (AW, POS, SE). Digital literacy moderated the AW → BI path slightly (interaction $\beta = 0.08$, $p = .045$), indicating employees with higher digital literacy convert awareness into intention more effectively.

Discussion

Key Findings and Theoretical Implications

The findings validate that cybersecurity awareness (H1), perceived organizational support (H2), and self-efficacy (H4) are robust predictors of employees' behavioral intention to adopt digital safety practices. Perceived severity (H3) exhibits an important indirect effect: employees who view threats as severe are more likely to feel capable (higher self-efficacy) and thus intend to act, consistent with Protection Motivation Theory.

The model's explanatory power ($R^2 = .62$) is substantial for behavioral intention in organizational settings, indicating that combined cognitive (awareness, severity), organizational (POS), and personal (self-efficacy) factors capture the bulk of employees' motivational drivers. These results affirm socio-cognitive and organizational perspectives on cybersecurity behavior (Ifinedo, 2012; Parsons et al., 2017).

Practical Implications for Telecom Firms

Practical takeaways are clear:

1. **Invest in awareness + skills**: Awareness campaigns should be coupled with practical, hands-on training to raise self-efficacy—not merely passive messaging. Scenario-based phishing drills, simulation environments, and guided configuration sessions build competence.
2. **Demonstrate organizational support**: Leadership must visibly prioritize security: allocate time for security tasks, provide tools that reduce cognitive load (password managers, single sign-on with 2FA), and reward compliance. POS enhances normative pressure and signals that security behaviors are valued.
3. **Frame severity constructively**: Communicating the seriousness of threats should be paired with clear, actionable steps so perceived severity does not paralyze employees; the pathway through self-efficacy must be reinforced.
4. **Tailor to literacy levels**: Employees with lower digital literacy benefit from incremental training and simpler workflows; nudges (micro-prompts, inline tips) help translate awareness into behavior.

Managerial Design Recommendations

- Adopt a blended training model (microlearning + simulations).
- Use automated nudges and friction-reducing tools (e.g., forced 2FA setup flows).
- Implement transparent incident-handling processes so employees feel supported when reporting suspicious events.
- Measure and publicize security KPIs at team level to create shared responsibility.

Limitations and Future Research

Limitations include cross-sectional data preventing causal assertions and reliance on self-reported intentions rather than observed behavior. Future research should:

- Implement longitudinal designs linking intervention(s) to observed behaviors (click rates on phishing simulations, reporting frequency).
- Explore cultural factors unique to Pakistan (power distance, hierarchical communication) that may shape POS effects.
- Test interventions (A/B trials) of training modalities to quantify efficacy differences.

Conclusion

Employees are a decisive line of defense in telecom cybersecurity. This study demonstrates that raising cybersecurity awareness, delivering tangible organizational support, and building employee self-efficacy are central to strengthening behavioral intentions for digital safety practices. Telecom management must shift from awareness-only programs to integrated strategies that combine skill building, leadership signaling, and workplace design to make safe behavior simple, supported, and sustained.

References

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Bandura, A. (1997). *Self-efficacy: The exercise of control*. W. H. Freeman.

Bolgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based explanations. *MIS Quarterly*, 34(3), 523–548. (Note: correct ref is Bulgurcu, Cavusoglu & Benbasat, 2010)

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingate, P., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems*, 18(2), 151–164. https://doi.org/10.1057/ejis.2009.9

Chen, R., & Zahedi, F. M. (2016). Individual acceptance of information security countermeasures: A theoretical model. *MIS Quarterly*, 40(1), 1–23.

Eisenberger, R., Huntington, R., Hutchison, S., & Sowa, D. (1986). Perceived organizational support. *Journal of Applied Psychology*, 71(3), 500–507. https://doi.org/10.1037/0021-9010.71.3.500

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors. *Heliyon*, 3(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

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. https://doi.org/10.1016/j.cose.2011.10.007