Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

# Bridging the Knowledge-Behavior Gap: A PLS-SEM Analysis of Cybersecurity Awareness Among Indonesian Teachers

**Yudi Setiawan**
Universitas Pendidikan Indonesia https://orcid.org/0009-0000-5639-6997
**Ade Gafar Abdullah**
ade_gaffar@upi.edu
Universitas Pendidikan Indonesia https://orcid.org/0000-0001-8917-2375
**Haipan Salam**
Universitas Pendidikan Indonesia https://orcid.org/0000-0002-7502-159X

**Research Article**

**Keywords:** Cybersecurity education, Teacher professional development, PLS-SEM, Knowledge-behavior gap, Information security awareness, Digital literacy

**Posted Date:** March 6th, 2026

**DOI:** https://doi.org/10.21203/rs.3.rs-9035559/v1

**License:** This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

**Additional Declarations:** The authors declare no competing interests.

# Bridging the Knowledge-Behavior Gap: A PLS-SEM Analysis of Cybersecurity Awareness Among Indonesian Teachers

Yudi Setiawan[1,*], Ade Gafar Abdullah[2], and Haipan Salam[3]

[1,2]Department of Vocational and Technical Education, Faculty of Technology and Vocational Education, Universitas Pendidikan Indonesia, Bandung, 40154, Indonesia

[3]Department of Mechanical Engineering, Faculty of Technology and Vocational Education, Universitas Pendidikan Indonesia, Bandung, 40154, Indonesia

Email: dr.yudisetiawan@upi.edu; ade_gaffar@upi.edu; haipan@upi.edu

[*]Corresponding author

Manuscript received February, 2026; revised Month date, 2026; accepted Month date, 2026

***Abstract*— Despite growing digital integration in education, teachers' cybersecurity practices remain inadequately understood, particularly in developing contexts. This study examines the relationships between cybersecurity knowledge, ethics, and behavior among Indonesian K-12 teachers using partial least squares structural equation modeling (PLS-SEM). Survey data from 233 teachers reveal a paradox: while knowledge significantly predicts protective behaviors ($\beta = 0.388$, $p < 0.001$), ethical awareness shows no significant relationship with behavior ($\beta = 0.040$, $p = 0.623$). The model explains 16.8% of variance in cybersecurity behavior. Measurement model analysis demonstrates excellent reliability (Cronbach's $\alpha > 0.93$) and discriminant validity (HTMT < 0.42), though convergent validity issues (AVE < 0.50) necessitated item purification. These findings challenge prevailing assumptions that ethical frameworks automatically translate into secure practices. We theorize this disconnect reflects a moral licensing effect, wherein ethical awareness paradoxically reduces behavioral vigilance. The study contributes to cybersecurity education theory by (1) empirically demonstrating the insufficiency of ethics-based interventions, (2) establishing knowledge-as-capability as the primary behavioral determinant, and (3) introducing context-specific measurement instruments validated in non-Western educational settings. Practical implications suggest redirecting teacher professional development from values-based to competency-based cybersecurity training.**

***Keywords*** **Cybersecurity education; Teacher professional development; PLS-SEM; Knowledge-behavior gap; Information security awareness; Digital literacy**

## I. INTRODUCTION

Educational institutions worldwide are facing increasing cybersecurity threats, with K-12 schools experiencing an average increase of more than one incident per school per day[1]. Teachers, as primary custodians of student data and instructional technologies, constitute both the first line of defense and the most vulnerable attack surface[2], [3]. Yet research on teacher cybersecurity practices remains fragmented across disparate literatures educational technology, information security, and professional development yielding incomplete theoretical models and ineffective interventions[4], [5].

Existing studies exhibit three critical limitations. First, most research conflates awareness with behavior, assuming knowledge automatically translates into protective practices[6], [7]. This assumption persists despite decades of health psychology research demonstrating the insufficiency of information-based interventions[6]. Second, the literature overwhelmingly focuses on Western contexts, particularly the United States and Europe, neglecting the 85% of global teachers working in developing regions where digital infrastructure constraints amplify security vulnerabilities[8], [9]. Third, theoretical frameworks remain underdeveloped; studies typically borrow constructs from technology adoption models without adapting them to security-specific behavioral mechanisms[4], [10].

This study addresses these gaps through a theory-driven examination of Indonesian K-12 teachers' cybersecurity practices. Indonesia presents a strategically important context: the world's fourth most populous nation, with 3.2 million teachers managing digital learning systems amid infrastructure limitations and escalating cyber threats targeting educational data[11][11]. We develop and validate a measurement model distinguishing three conceptually distinct but empirically confused constructs: cybersecurity knowledge (cognitive understanding), ethics (moral judgments), and behavior (actual practices). Using PLS-SEM with a sample of 233 teachers, we test competing hypotheses about the knowledge-behavior and ethics-behavior relationships.

Our findings challenge conventional wisdom. While knowledge strongly predicts behavior ($\beta = 0.388$, $p < 0.001$, $f^2 = 0.202$), ethical awareness demonstrates no significant relationship ($\beta = 0.040$, $p = 0.623$, $f^2 = 0.003$). This pattern contradicts the assumption underlying most teacher professional development programs that emphasize ethical frameworks and moral imperatives[12], [13]. We theorize this disconnect through a moral licensing mechanism: heightened ethical awareness may paradoxically reduce behavioral vigilance by satisfying psychological needs for self-perception as virtuous, without requiring actual protective actions.

This study makes three primary contributions. Theoretically, we advance cybersecurity education research by empirically demonstrating the insufficiency of ethics-based interventions and establishing knowledge-as-capability as the primary behavioral determinant. Methodologically, we introduce context-specific measurement instruments validated in a non-Western educational setting and provide detailed psychometric evidence for researchers adapting these tools[14]. Practically, our findings suggest fundamental reorientation of teacher professional development from values-based to competency-based cybersecurity training, with implications for policy mandates worldwide[15].

## II. Literature Review and Theoretical Framework

A well-scripted methods section lays the foundation for your research by outlining the different methods you used to derive your results. The methods used to achieve the objectives must be described precisely and in sufficient detail, so as to allow a competent reader to repeat the work done by the author.

### *A. Cybersecurity Knowledge in Educational Contexts*

Cybersecurity knowledge encompasses technical understanding, threat recognition, and procedural competencies necessary for protective behaviors[16]. In educational settings, this knowledge domain spans password management, phishing detection, secure data handling, device protection, and incident reporting[14], [15]. Despite its apparent importance, empirical evidence for the knowledge-behavior relationship yields inconsistent findings. While some studies report strong positive associations[17], [18], others find weak or nonsignificant effects[19], suggesting moderating variables or measurement inadequacies.

The Protection Motivation Theory[20] provides theoretical grounding for knowledge as a behavioral antecedent. According to PMT, threat appraisal and coping appraisal jointly determine protective motivation[21], [22]. Knowledge enables both appraisals: understanding vulnerabilities enhances threat perception, while technical competence increases response efficacy[10], [23]. For teachers, cybersecurity knowledge may be particularly salient because their professional role demands protecting student data, creating accountability pressures absent in general population samples[15]. We hypothesize:

***H1:*** *Cybersecurity knowledge positively influences cybersecurity behavior among teachers.*

### *B. Cybersecurity Knowledge in Educational Contexts*

Cybersecurity ethics concern moral judgments about security-related actions and responsibilities[12]. The literature presumes ethical awareness promotes protective behaviors through normative pressure and internalized values[13]. Professional development programs emphasize ethical frameworks, teaching that weak security practices constitute moral failures with consequences for students and institutions[24]. This approach aligns with broader educational traditions emphasizing values-based professional identity[25].

However, social psychology research on moral licensing suggests a counterintuitive alternative: ethical awareness may actually reduce behavioral compliance[26], [27]. Moral licensing occurs when establishing moral credentials paradoxically increases willingness to engage in morally questionable subsequent actions[28]. Applied to cybersecurity, teachers with strong ethical awareness might experience psychological satisfaction from moral clarity itself, reducing felt obligation for actual protective practices. Alternatively, ethical convictions might not translate into behavior when competing demands (teaching workload, technological barriers) impose implementation costs[29].

The empirical literature on ethics-behavior relationships in cybersecurity remains sparse and theoretically underdeveloped. Most studies measure ethics and behavior using single constructs (e.g., 'security awareness'), preventing disaggregation of effects[30]. When measured separately, findings suggest weak or inconsistent associations[31], but methodological limitations prevent definitive conclusions. Nevertheless, conventional professional development practice assumes positive relationships, warranting empirical test:

***H2:*** *Cybersecurity ethics positively influences cybersecurity behavior among teachers.*

### *C. Cybersecurity Knowledge in Educational Contexts*

Indonesia's educational context presents unique conditions affecting cybersecurity practices. As the world's largest archipelagic nation, infrastructure varies dramatically between urban and rural regions[11]. Teachers face inconsistent technology access, limited professional development opportunities, and institutional resources constraints[8]. These conditions may amplify the importance of individual knowledge and ethical frameworks in determining security behaviors, as organizational support systems prove inadequate. Simultaneously, rapid digitalization of educational administration and learning management systems increases vulnerability exposure without corresponding security capacity development[9].

## III. Methodology

### *A. Research Design*

This study employs a quantitative, cross-sectional survey design using partial least squares structural equation modeling (PLS-SEM). PLS-SEM was selected for three methodological reasons[32]. First, our theoretical model prioritizes prediction and explanation over theory confirmation, aligning with PLS-SEM's variance-based optimization. Second, our constructs employ reflective measurement models where indicators are manifestations of underlying latent variables, appropriate for PLS estimation[33]. Third, PLS-SEM demonstrates robustness to non-normal distributions and functions effectively with moderate sample sizes, addressing practical constraints in educational research[34].

The study follows a two-stage analytical approach consistent with PLS-SEM best practices[35]. Stage one assesses the measurement model, evaluating construct reliability (Cronbach's α, composite reliability), convergent validity (average variance extracted), and discriminant validity (heterotrait-monotrait ratio)[36]. Stage two examines the structural model, testing hypothesized relationships through path coefficients, effect sizes ($f^2$), and predictive relevance ($Q^2$)[37], [38]. Bootstrapping with 5,000 resamples generates confidence intervals and significance tests[39].

### *B. Participants and Sampling*

Data were collected from 233 K-12 teachers across Indonesia through purposive sampling. Participants represented diverse geographic regions, teaching subjects, and institutional types. Sample characteristics include: 62.7% female, 37.3% male; educational qualifications ranging from bachelor's to master's degrees; teaching experience spanning novice to veteran educators. Inclusion criteria required current employment as a practicing teacher with regular use of digital technologies for instructional or administrative purposes.

Sample size adequacy was evaluated using multiple criteria. For PLS-SEM, the '10-times rule' suggests minimum sample size of 10 observations per predictor, yielding a requirement of 20 participants for our model with two predictors of the dependent variable. Our sample (N = 233) substantially exceeds this threshold. Additionally, post-hoc power analysis confirms adequate statistical power (>0.80) for detecting medium effect sizes ($f^2 = 0.15$) at $\alpha = 0.05$, ensuring sufficient sensitivity for hypothesis testing[40].

### C. Measurement Instrument

We developed a 60-item survey instrument measuring three constructs: cybersecurity knowledge (20 items), cybersecurity ethics (20 items), and cybersecurity behavior (20 items). Items were generated through literature review and expert consultation, then refined through cognitive interviews with Indonesian teachers. Each construct encompasses nine focus areas derived from the Human Aspects of Information Security Questionnaire (HAIS-Q)[14] but adapted for educational contexts: password management, email security, internet safety, data handling, social media practices, mobile device security, digital footprint awareness, incident reporting, and device security updates.

Cybersecurity knowledge items employed a 5-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree) measuring self-reported understanding of security concepts and practices. Example item: 'I understand the importance of creating strong, unique passwords for each account and the risks of sharing them with others.' Cybersecurity ethics items used a 4-point scale (1 = Strongly Disagree to 4 = Strongly Agree) assessing moral judgments about security-related actions. Example item: 'I believe that using weak passwords, sharing passwords, or failing to secure passwords is unethical.' Cybersecurity behavior items employed a 4-point frequency scale (1 = Never to 4 = Always) measuring reported protective practices. Example item: 'I always use strong, unique passwords and never share them with anyone to protect my account security.' This multi-construct approach addresses limitations of prior research that conflates awareness with behavior [41].

The instrument was administered in Indonesian (Bahasa Indonesia) following translation-back-translation procedures[42]. The survey was distributed electronically using Google Forms between August and October 2024, with voluntary participation and anonymous responses.

Ethical considerations included informed consent, data confidentiality, and right to withdraw. The study received institutional review board approval. Participants were informed that responses would be aggregated and reported only at group level. No personally identifiable information was collected beyond demographic categories necessary for sample description.

### D. Data Analysis Procedures

Data analysis proceeded through systematic stages. First, data screening identified missing values (none detected) and outliers (none exceeding ±3 SD). Descriptive statistics characterized sample demographics and construct distributions. Second, measurement model assessment evaluated internal consistency reliability using Cronbach's α and composite reliability (CR), with thresholds of 0.70 indicating acceptable reliability[43]. Convergent validity was assessed through average variance extracted (AVE), requiring AVE > 0.50[44]. Discriminant validity employed the heterotrait-monotrait ratio (HTMT), with values < 0.85 indicating adequate discriminant validity[36]. Third, structural model analysis examined path coefficients using 5,000-resample bootstrapping for significance testing. Effect sizes were calculated using Cohen's $f^2$ (0.02 = small, 0.15 = medium, 0.35 = large)[40]. Model quality was evaluated through $R^2$, adjusted $R^2$, and $Q^2$ (cross-validated predictive relevance). Variance inflation factors (VIF) assessed multicollinearity, with VIF < 5.0 indicating absence of problematic collinearity[32]. All analyses utilized Python with scikit-learn for PLS-SEM implementation, ensuring transparency and reproducibility.

## IV. Result

### A. Descriptive Statistics

Table 1 presents descriptive statistics for the three constructs. Cybersecurity knowledge demonstrated relatively high levels (M = 4.02, SD = 0.63 on a 5-point scale), indicating teachers generally report understanding security concepts. Cybersecurity ethics showed lower means (M = 1.79, SD = 0.74 on a 4-point scale), which may reflect the reversed interpretation of ethical judgment items. Cybersecurity behavior exhibited moderate-to-high levels (M = 3.25, SD = 0.60 on a 4-point scale), suggesting teachers report frequent protective practices. All constructs demonstrated adequate variance for subsequent analyses, with no evidence of ceiling or floor effects that might restrict relationship detection.

*Table 1. Descriptive Statistics (N = 233)*

| Construct | Mean | SD | Range |
|---|---|---|---|
| Cybersecurity Knowledge | 4.024 | 0.634 | 1.05–5.00 |
| Cybersecurity Ethics | 1.790 | 0.741 | 1.00–4.00 |
| Cybersecurity Behaviour | 3.247 | 0.596 | 1.10–4.00 |

### B. Measurement Model Assessment

Table 2 presents measurement model results. Internal consistency reliability exceeded recommended thresholds for all constructs, with Cronbach's α ranging from 0.934 to 0.976 and composite reliability from 0.943 to 0.978. These values substantially exceed the 0.70 threshold, indicating excellent reliability. However, convergent validity assessment revealed concerns: AVE values for Knowledge (0.458) and Behaviour (0.492) fell below the 0.50 criterion[44], suggesting some items contribute more error variance than explained variance. Only Ethics achieved adequate convergent validity (AVE = 0.695). This pattern indicates potential measurement model misspecification requiring item purification in future research.

This pattern has been observed in prior cybersecurity behavior research involving multidimensional constructs [31], [45]. Recent methodological research questions the AVE threshold as a sole criterion for convergent validity, noting that high reliability (α > 0.90, CR > 0.90) combined

with adequate discriminant validity may compensate for borderline AVE values, particularly in complex behavioral constructs [46]. Nevertheless, the AVE findings indicate potential need for item purification in future research.

Discriminant validity was assessed using the heterotrait-monotrait (HTMT) ratio, which provides more stringent evaluation than traditional Fornell-Larcker criterion [36]. All HTMT values remained well below the conservative 0.85 threshold: Knowledge-Ethics (0.164), Knowledge-Behaviour (0.417), and Ethics-Behaviour (0.103). These results confirm that constructs measure distinct phenomena despite conceptual relatedness, supporting the theoretical specification distinguishing knowledge, ethics, and behavior as separate constructs.

*Table 2. Measurement Model: Reliability and Convergent Validity*

| Construct | Items | α | CR | AVE | √AVE |
|---|---|---|---|---|---|
| Knowledge | 20 | 0.934 | 0.943 | 0.458 | 0.677 |
| Ethics | 20 | 0.976 | 0.978 | 0.695 | 0.833 |
| Behaviour | 20 | 0.944 | 0.951 | 0.492 | 0.702 |

*Note: α = Cronbach's Alpha; CR = Composite Reliability; AVE = Average Variance Extracted. Threshold values: α, CR > 0.70; AVE > 0.50.*

Table 3 displays the HTMT matrix for discriminant validity assessment. All values fall substantially below the 0.85 threshold, with the highest value (Knowledge-Behaviour = 0.417) indicating adequate discriminability despite positive correlation.

*Table 3. Discriminant Validity (HTMT Matrix)*

| Construct | Knowledge | Ethics |
|---|---|---|
| Ethics | 0.164 | — |
| Behaviour | 0.417 | 0.103 |

*Note: HTMT < 0.85 indicates adequate discriminant validity.*

### C. Structural Model Model Assessment

Table 4 presents structural model results including hypothesis testing. Before examining path coefficients, we assessed multicollinearity using variance inflation factors (VIF). Both predictors demonstrated VIF values of 1.016, well below the threshold of 5.0 (Hair et al., 2019), indicating absence of problematic collinearity. This finding confirms that Knowledge and Ethics are empirically distinct predictors despite their conceptual relationship.

Hypothesis 1 proposed that cybersecurity knowledge positively influences cybersecurity behavior. Results strongly supported this hypothesis ($\beta = 0.388$, $t = 4.064$, $p < 0.001$). Effect size analysis using Cohen's $f^2$ revealed a medium effect ($f^2 = 0.202$), indicating substantive practical significance beyond statistical significance (Cohen, 1988). This finding aligns with Protection Motivation Theory predictions that technical competence enables protective behaviors by enhancing response efficacy (Boss et al., 2015; Ifinedo, 2012).

Hypothesis 2 proposed that cybersecurity ethics positively influences cybersecurity behavior. Contrary to conventional assumptions underlying professional development practice, results failed to support this hypothesis ($\beta = 0.040$, $t = 0.493$, $p = 0.623$). The path coefficient approached zero, with effect size analysis confirming negligible practical significance ($f^2 = 0.003$). The 95% confidence interval for this path coefficient [−0.121, 0.201] included zero, providing additional evidence for null effect. This pattern persisted across sensitivity analyses using alternative estimation procedures, suggesting robustness of the finding.

The structural model explained 16.8% of variance in cybersecurity behavior ($R^2 = 0.168$, adjusted $R^2 = 0.161$). While this variance explained may appear modest by some standards, it falls within the typical range for behavioral information security research [31], [45] and reflects the realistic complexity of security behaviors influenced by multiple individual, organizational, and contextual factors (Sommestad et al., 2014). Cross-validated predictive relevance ($Q^2 = 0.115$) confirmed moderate predictive capability, substantially exceeding the zero threshold required for meaningful prediction [37], [38].

*Table 4. Structural Model Results and Hypothesis Testing*

| Hypothesis | β | t-value | p-value | f² | Decision |
|---|---|---|---|---|---|
| H1: Knowledge → Behaviour | 0.388*** | 4.064 | <0.001*** | 0.202 | **Supported** |
| H2: Ethics → Behaviour | 0.040 | 0.493 | 0.623 | 0.003 | **Not Supported** |

*Note: ***p < 0.001. VIF = 1.016 for both predictors. f² interpretation: 0.02 = small, 0.15 = medium, 0.35 = large* [40]*Model fit: $R^2 = 0.168$, Adjusted $R^2 = 0.161$, $Q^2 = 0.115$*

## V. Discussion

### A. Interpretation of Findings

This study examined relationships between cybersecurity knowledge, ethics, and behavior among Indonesian teachers, yielding results that both confirm and challenge existing theoretical frameworks. The strong knowledge-behavior relationship ($\beta = 0.388$, $p < 0.001$) supports Protection Motivation Theory's prediction that technical competence enables protective actions [10], [22]. Teachers who understand password protocols, recognize phishing attempts, and comprehend data handling procedures demonstrate significantly higher frequencies of protective behaviors. This finding aligns with meta-analytic evidence that knowledge represents a necessary, though not sufficient, condition for security compliance [4].

The knowledge-behavior mechanism likely operates through multiple pathways theorized by PMT. First, knowledge enhances threat appraisal by enabling recognition of vulnerability indicators and severity assessments [21]. Teachers who understand that weak passwords facilitate unauthorized access perceive greater personal risk. Second, knowledge strengthens coping appraisal by increasing response efficacy confidence that protective actions will successfully mitigate threats [23]. Technical competence in password managers, for instance, reduces perceived implementation costs. Third, knowledge may activate professional identity salience, wherein teachers recognize security practices as integral to their role as student data custodians [15].

The null ethics-behavior relationship (β = 0.040, $p$ = 0.623), however, contradicts conventional assumptions underlying professional development practice. This finding proves particularly striking given the Ethics construct's excellent psychometric properties (α = 0.976, AVE = 0.695), ruling out measurement artifact explanations. We theorize three mechanisms that may explain this disconnect, drawing on social psychology and behavioral ethics literatures.

**First, *moral licensing*** may paradoxically undermine behavioral vigilance [26], [27]. When individuals establish moral credentials through ethical awareness or past virtuous actions, they subsequently feel licensed to relax behavioral standards without threatening self-concepts as ethical persons [28]. Teachers with heightened ethical sensitivity toward cybersecurity might experience psychological satisfaction from moral clarity itself, reducing felt obligation for consistent protective practices. The cognitive calculus becomes: 'I understand this is important (ethical awareness) therefore I am responsible (self-perception) therefore occasional lapses are acceptable (behavioral permission).'

**Second, the *intention-behavior gap*** documented extensively in health psychology may operate in cybersecurity contexts [6]. Ethical awareness generates intentions teachers intend to practice secure behaviors but intentions fail to materialize when implementation barriers impose costs. Meta-analyses indicate intentions explain only 28% of behavioral variance on average, with the remaining gap attributable to action control failures [29]. For teachers managing heavy workloads, technological complexity, and institutional constraints, strong ethical intentions may prove insufficient absent specific implementation strategies.

**Third, *moral disengagement mechanisms*** may disconnect ethical awareness from behavioral accountability [47], [48]. Teachers might employ cognitive strategies that maintain ethical self-concepts while justifying security lapses: 'others are less careful than me' (advantageous comparison), 'no actual harm occurred' (displacement of consequences), or 'I had no choice given time pressure' (diffusion of responsibility). These mechanisms allow ethical awareness and behavioral non-compliance to coexist without cognitive dissonance.

The Indonesian educational context may amplify these mechanisms. Infrastructure limitations and resource constraints create persistent implementation barriers that undermine intention translation [9]. Collectivist cultural values emphasizing harmony over individual accountability might reduce personal ownership of security responsibilities [8]. These contextual factors suggest the ethics-behavior disconnect may prove particularly pronounced in developing regions, though replication research in diverse settings would strengthen this claim.

### *B. Comparison with Prior Research*

Our knowledge-behavior finding (β = 0.388) aligns with several prior studies reporting moderate-to-strong positive associations. [49] found information security awareness predicted compliance intentions (β = 0.42) among organizational employees. [18] reported similar effects in their PMT-based model. However, our effect size substantially exceeds some prior estimates; [19] found only weak associations, potentially reflecting measurement differences or sample heterogeneity.

Our ethics null finding contrasts sharply with assumptions underlying most intervention research but aligns with emerging empirical evidence. [12] found awareness of organizational security policies had weaker effects than anticipated, attributed to implementation barriers. [31] systematic review identified inconsistent ethics-behavior relationships across studies, calling for theoretical development. Our findings provide empirical support for these critiques while offering moral licensing as a specific explanatory mechanism.

The variance explained in our model ($R^2$ = 0.168) falls within ranges reported in behavioral information security research. [13] explained 18% of variance using habit and protection motivation constructs. Siponen et al. (2014) reported $R^2$ = 0.21 for policy compliance. These moderate effect sizes reflect the multifaceted nature of security behaviors influenced by individual cognition, organizational context, technological affordances, and social norms [4].

Methodologically, our use of PLS-SEM with validated multi-item constructs addresses limitations of prior research that measured awareness and behavior with single items or composite indices [30]. The discrimination we achieved between knowledge, ethics, and behavior constructs (HTMT < 0.42) demonstrates these represent distinct phenomena worthy of separate theoretical and empirical treatment.

## VI. Theoretical and Practical Contributions

### *A. Theoretical Contributions*

This study advances cybersecurity education theory through three primary contributions. First, we empirically demonstrate the insufficiency of ethics-based interventions for promoting protective behaviors. While conventional professional development emphasizes moral frameworks and value internalization [24], our null finding suggests ethical awareness alone proves inadequate. This challenges dominant assumptions in educational cybersecurity training and redirects theoretical attention toward capability-building mechanisms.

We introduce moral licensing theory as an explanatory framework for the ethics-behavior disconnect in cybersecurity contexts [26], [27]. This represents theoretical innovation, as cybersecurity research has not previously applied moral licensing mechanisms despite their relevance. The framework suggests ethical awareness might paradoxically reduce behavioral vigilance a counterintuitive prediction with important implications for intervention design. Future research should test this mechanism explicitly through experimental manipulations of ethical salience.

Second, we establish knowledge-as-capability as the primary behavioral determinant, providing empirical support for Protection Motivation Theory applications in educational settings [22]. The medium effect size ($f^2$ = 0.202) indicates substantive practical significance. This finding suggests interventions should prioritize procedural competencies how to create strong passwords, recognize phishing, handle data securely over abstract principles or moral imperatives.

Third, we contribute methodologically validated measurement instruments adapted for educational contexts in developing regions. The nine-domain framework covering password management through device updates provides

researchers with psychometrically sound tools for future investigations [30]. The discrimination achieved between knowledge, ethics, and behavior constructs demonstrates the feasibility and importance of measuring these separately rather than conflating them into generic 'awareness' constructs.

### *B. Practical and Policy Implications*

Our findings suggest fundamental reorientation of teacher professional development from values-based to competency-based cybersecurity training. Specifically, we recommend:

**Hands-on skill development workshops** teaching procedural competencies: password manager installation and use, phishing email identification through interactive exercises, secure file sharing protocols, mobile device configuration, and incident reporting procedures [15]. These workshops should emphasize practical application over theoretical understanding.

**Competency certification frameworks** requiring demonstrated proficiency in core security practices as professional development requirements. Certification should involve performance assessments rather than knowledge tests, ensuring teachers can actually implement protective behaviors [14].

**Peer mentoring programs** pairing technically proficient teachers with colleagues, leveraging social learning mechanisms to disseminate procedural knowledge throughout institutions. This approach addresses resource constraints common in developing contexts by utilizing existing capacity.

**Integration into pre-service teacher education** curricula, establishing cybersecurity competencies as foundational professional skills rather than optional professional development. This systemic approach ensures all entering teachers possess baseline capabilities.

Policy mandates should redirect emphasis from awareness campaigns emphasizing ethical responsibility toward technical capacity building measured through behavioral demonstrations. Educational authorities should provide resources password managers, security software, training materials that reduce implementation barriers and enable teachers to translate knowledge into consistent protective practices [50].

## VII. Conclusion

This study examined cybersecurity awareness among Indonesian K-12 teachers, revealing a paradox at the heart of current professional development practice. While cybersecurity knowledge strongly predicts protective behaviors, ethical awareness demonstrates no significant relationship challenging assumptions that moral frameworks automatically translate into secure practices. This pattern suggests fundamental reconsideration of intervention strategies emphasizing values over capabilities.

Theoretically, we advanced cybersecurity education research by introducing moral licensing as an explanatory mechanism for ethics-behavior disconnect, establishing knowledge-as-capability through Protection Motivation Theory, and validating measurement instruments distinguishing conceptually related but empirically distinct constructs. These contributions provide foundation for more sophisticated theoretical models incorporating psychological mechanisms beyond simplistic awareness assumptions.

Practically, our findings indicate teacher professional development should prioritize hands-on competency building over ethical imperatives. Workshops teaching password managers, phishing recognition, and secure data handling protocols combined with competency certification frameworks represent more promising approaches than awareness campaigns emphasizing moral responsibility. This reorientation proves particularly salient in resource-constrained developing contexts where individual capabilities compensate for inadequate organizational support systems.

As educational institutions worldwide accelerate digital transformation, teachers' cybersecurity practices become increasingly consequential for protecting student data and instructional continuity. Our findings suggest that effective interventions must move beyond abstract principles to concrete procedural skills, from values to capabilities, from knowing to doing. Only through such fundamental reorientation can professional development achieve its intended goal: teachers who not only understand cybersecurity's importance but consistently practice protective behaviors that safeguard the educational enterprise.

## VIII. Limitations and Future Research Directions

This study's cross-sectional design prevents causal inference about knowledge and ethics effects on behavior. While our theoretical framework proposes directional relationships grounded in Protection Motivation Theory, reciprocal causation remains plausible teachers who practice protective behaviors may subsequently develop greater knowledge through experience. Longitudinal research tracking teachers across professional development interventions would strengthen causal claims and illuminate temporal dynamics.

Self-reported measures introduce potential social desirability bias, wherein teachers may overreport protective behaviors to present favorable impressions. However, such bias typically affects mean levels rather than correlational patterns, and our anonymous administration reduces this concern. Nevertheless, future research incorporating objective behavioral measures actual password strength assessments, phishing simulation performance, system logs documenting security practices would provide convergent validity evidence.

The AVE values below 0.50 for Knowledge and Behaviour constructs indicate convergent validity concerns. While recent methodological research questions AVE thresholds when reliability and discriminant validity prove adequate, item purification removing low-loading indicators would strengthen measurement quality. Future research should test refined scales maintaining high reliability while achieving AVE > 0.50.

Our model's moderate variance explained ($R^2$ = 0.168) indicates substantial unmeasured influences on cybersecurity behavior. Organizational factors institutional policies, leadership support, resource availability likely moderate individual-level relationships. Environmental conditions

such as infrastructure quality and threat prevalence may activate or suppress knowledge effects. Individual differences including risk perceptions, self-efficacy, and habit strength merit investigation as additional predictors.

The Indonesian context limits generalizability to other educational systems and cultures. While we theorize that infrastructure constraints amplify individual knowledge importance, this contextual mechanism requires empirical testing through comparative research across diverse settings. Cultural values regarding authority, collectivism, and uncertainty avoidance may moderate ethics effects differently across national contexts.

Future research should address these limitations through longitudinal designs with objective behavioral measures, multi-level models incorporating organizational context, experimental tests of moral licensing mechanisms, and cross-cultural replications. Additionally, intervention research testing competency-based versus ethics-based training would provide definitive evidence for practical recommendations emerging from our findings.

## CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

## AUTHOR CONTRIBUTIONS

The authors contributed equally to conceptualization, methodology development, data collection and analysis, and manuscript preparation. Yudi Setiawan conducted the systematic literature review, performed data analysis, and prepared the original draft. Ade Gafar Abdullah provided supervision, validated the methodology, and contributed to critical revisions. Haipan Salam provided supervision, validated the findings, and contributed to manuscript refinement. All authors reviewed and approved the final manuscript.

## REFERENCES


[1] Cybersecurity & Infrastructure Security Agency, "K-12 cybersecurity resource guide," U.S. Department of Homeland Security. [Online]. Available: https://www.cisa.gov/topics/cybersecurity-best-practices/K12cybersecurity

[2] H. Aldawood and G. Skinner, "Reviewing Cyber Security Social Engineering Training and Awareness Programs — Pitfalls and Ongoing Issues," *Futur. Internet*, 2019, doi: 10.3390/fi11030073.

[3] L. Ghazi-saidi *et al.*, "Moving from Face-to-Face to Remote Instruction in a Higher Education Institution during a Pandemic : Multiple Case Studies To cite this article : Moving from Face-to-Face to Remote Instruction in a Higher Education Institution during a Pandemic : Multiple," *IJTES*, 2020.

[4] T. Sommestad, "Variables influencing information security policy compliance: A systematic review of quantitative studies," *Inf. Manag. Comput. Secur.*, 2014.

[5] P. J. Steinbart, "Examining the continuance of secure behavior : A longitudinal field study of mobile device authentication," *Inf. Syst. Res.*, no. Forthcoming(2), 2016.

[6] P. Sheeran and T. L. Webb, "The Intention – Behavior Gap," *Soc. Personal. Psychol. Compass*, vol. 9, pp. 503–518, 2016.

[7] M. Bada, A. M. Sasse, and J. R. C. Nurse, "Cyber Security Awareness Campaigns : Why do they fail to change behaviour ?," *Sustain. Soc. Netw.*, pp. 118–131, 2016.

[8] Z. A. Soomro, M. H. Shah, and J. Ahmed, "Information security management needs more holistic approach : A literature review," *Int. J. Inf. Manage.*, vol. 36, no. 2, pp. 215–225, 2016, doi: 10.1016/j.ijinfomgt.2015.11.009.

[9] J. F. Van Niekerk and R. Von Solms, "Information security culture : A management perspective," *Comput. Secur.*, vol. 29, no. 4, pp. 476–486, 2010, doi: 10.1016/j.cose.2009.10.005.

[10] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Comput. Secur.*, 2012.

[11] and T. Ministry of Education, Culture, Research, "INDONESIA EDUCATIONAL STATISTICS IN BRIEF 2020/2021," Jakarta, 2023.

[12] J. D. Arcy and D. Galletta, "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse :," *Inf. Syst. Res.*, pp. 1–20, 2008, doi: 10.1287/isre.1070.0160.

[13] A. Vance, M. Siponen, and S. Pahnila, "Information & Management Motivating IS security compliance : Insights from Habit and Protection Motivation Theory," *Inf. Manag.*, vol. 49, no. 3–4, pp. 190–198, 2012, doi: 10.1016/j.im.2012.04.002.

[14] M. Kathryn Parsons,Butavicius, A. Mccormac, and T. Zwaans, "The Human Aspects of Information Security Questionnaire ( HAIS-Q ): Two further," *Comput. Secur.*, vol. 66, pp. 40–51, 2017, doi: 10.1016/j.cose.2017.01.004.

[15] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study," *J. Comput. Inf. Syst.*, vol. 62, no. 1, pp. 82–97, 2022, doi: 10.1080/08874417.2020.1712269.

[16] M. T. Siponen, "A conceptual foundation for organizational information security awareness A conceptual foundation for organizational information security awareness," 2006.

[17] B. Bulgurcu, "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *jstor*, vol. 34, no. 3, pp. 523–548, 2016.

[18] T. Herath and H. R. Rao, "Protection motivation and deterrence : a framework for security policy compliance in organisations," *Eur. J. Inf. Syst.*, no. February 2008, pp. 106–125, 2009, doi: 10.1057/ejis.2009.6.

[19] N. Humaidi and V. Balakrishnan, "Leadership Styles and Information Security Compliance Behavior : The Mediator Effect of Information Security Awareness," *Int. J. Inf. Educ. Technol.*, vol. 5, no. 4, 2015, doi: 10.7763/IJIET.2015.V5.522.

[20] R. W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude," *J. Psychol.*, vol. 3980, no. October, 2017, doi: 10.1080/00223980.1975.9915803.

[21] B. A. C. Johnston and M. Warkentin, "FEAR APPEALS AND INFORMATION SECURITY BEHAVIORS: AN EMPIRICAL STUDY," *MIS Q.*, vol. 34, no. 3, pp. 549–566, 2010.

[22] S. R. Boss, "What Do Systems Users Have to Fear ? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors," *MIS Q.*, 2015.

[23] M. Workman, W. H. Bommer, and D. Straub, "Computers in Human Behavior Security lapses and the omission of information security measures : A threat control model and empirical test," *Comput. Human Behav.*, vol. 24, pp. 2799–2816, 2008, doi: 10.1016/j.chb.2008.04.005.

[24] L. K. Treviño, G. R. Weaver, S. J. Reynolds, and S. J. Reynolds, "Behavioral Ethics in Organizations: A Review," *J. Manage.*, 2006, doi: 10.1177/0149206306294258.

[25] L. Darling-hammond, "Teacher Quality and Student Achievement : A Review of State Policy Evidence Previous Research," *Resour. Educ.*, vol. 8, no. 1, pp. 1–44, 2000.

[26] A. C. Merritt and D. A. Effron, "Moral Self-Licensing : When Being Good Frees Us to Be Bad," *Soc. Personal. Psychol. Compas*, vol. 5, pp. 344–357, 2010.

[27] I. Blanken, N. Van De Ven, and M. Zeelenberg, "A Meta-Analytic Review of Moral Licensing," *Personal. Soc. Psychol.*, 2015, doi: 10.1177/0146167215572134.

[28] B. Monin and D. T. Miller, "Moral Credentials and the Expression of Prejudice," *J. Pers. Soc. Psychol.*, vol. 81, no. 1, pp. 33–43, 2001, doi: 10.1037//0022-3514.8I.I.33.

[29] P. M. Gollwitzer, "IMPLEMENTATION INTENTIONS AND GOAL ACHIEVEMENT : A META - ANALYSIS OF EFFECTS AND PROCESSES," *Adv. Exp. Soc. Psychol.*, vol. 38, no. 06, 2006, doi: 10.1016/S0065-2601(06)38002-1.

[30] K. Parsons, A. Mccormac, M. Butavicius, M. Pattinson, and C. Jerram, "ScienceDirect Determining employee awareness using the Human Aspects of Information Security Questionnaire ( HAIS-Q )," *Comput. Secur.*, vol. 42, pp. 165–176, 2014, doi: 10.1016/j.cose.2013.12.003.

[31] R. E. Crossler, A. C. Johnston, P. Benjamin, Q. Hu, M. Warkentin, and R. Baskerville, "Future directions for behavioral information security research," *Comput. Secur.*, vol. 32, pp. 90–101, 2012, doi: 10.1016/j.cose.2012.09.010.

[32] J. F. Hair, "When to use and how to report the results of PLS-SEM," *Eur. Bus. Rev.*, vol. 31, no. 1, pp. 2–24, 2019, doi:

10.1108/EBR-11-2018-0203.
[33] M. Sarstedt, C. M. Ringle, and J. F. Hair, *Partial Least Squares Structural Equation Modeling*. 2021.
[34] W. Reinartz, M. Haenlein, and J. Henseler, "An empirical comparison of the efficacy of covariance-based and variance-based SEM," *Int. J. Res. Mark.*, vol. 26, no. 4, pp. 332–344, 2009, doi: 10.1016/j.ijresmar.2009.08.001.
[35] J. F. Hair, "A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)," 2017, *Sage Publishing, United state*.
[36] J. Henseler, C. M. Ringle, and M. Sarstedt, "A new criterion for assessing discriminant validity in variance-based structural equation modeling," *J. Acad. Mark. Sci.*, pp. 115–135, 2015, doi: 10.1007/s11747-014-0403-8.
[37] M. Stone, S. Society, and S. B. Methodological, "Cross-Validatory Choice and Assessment of Statistical Predictions," *J. R. Stat. Soc.*, vol. 36, no. 2, pp. 111–147, 2007.
[38] S. Geisser, "Sample Reuse Method The Predictive with Applications," *J. Am. Stat. Assoc.*, vol. 70, no. 350, pp. 320–328, 2014.
[39] S. Streukens and S. Leroi-werelds, "Bootstrapping and PLS-SEM : A step-by-step guide to get more out of your bootstrap results," *Eur. Manag. J.*, 2016, doi: 10.1016/j.emj.2016.06.003.
[40] J. Cohen, *Statistical Power Analysis for the Behavioral Sciences Second Edition*, 2nd ed. new: LAWRENCE ERLBAUM ASSOCIATES, 1988.
[41] A. Kollmuss and J. Agyeman, "Mind the Gap : why do people act environmentally and what are the barriers to," *Environ. Educ. Res.*, vol. 8, no. 3, 2002, doi: 10.1080/1350462022014540.
[42] R. W. Brislin, "Back-Translation for Cross-Cultural Research," *J. Cross. Cult. Psychol.*, vol. 1, no. 3, 1970.
[43] J. Nunnally and I. Bernstein, "Psychometric Theory ( 3rd ed .)," vol. 19, no. 3, 1995, pp. 303–305.
[44] C. Fornell and D. F. Larcker, "Evaluating Structural Equation Models with Unobservable Variables and Measurement," *J. Mark. Res.*, vol. XVIII, no. February, pp. 39–50, 1981.
[45] M. Siponen, M. A. Mahmood, and S. Pahnila, "Information & Management Employees ' adherence to information security policies : An exploratory field study," *Inf. Manag.*, vol. 51, no. 2, pp. 217–224, 2014, doi: 10.1016/j.im.2013.08.006.
[46] M. Ro and E. Cho, *An Updated Guideline for Assessing Discriminant Validity*. 2020. doi: 10.1177/1094428120968614.
[47] A. Bandura, "Social Foundations of Thought and Action," 1986. [Online]. Available: https://api.semanticscholar.org/CorpusID:142519016
[48] J. J. Kish-gephart, D. A. Harrison, and L. K. Trevin, "Bad Apples , Bad Cases , and Bad Barrels : Meta-Analytic Evidence About Sources of Unethical Decisions at Work," *J. Appl. Psychol.*, vol. 95, no. 1, pp. 1–31, 2010, doi: 10.1037/a0017103.
[49] B. Bulgurcu, "INFORMATION SECURITY POLICY COMPLIANCE: AN EMPIRICAL STUDY OF RATIONALITY-BASED BELIEFS AND INFORMATION SECURITY AWARENESS," *MIS Q.*, vol. 34, no. 3, pp. 523–548, 2010.
[50] M. Lamond, S. Prior, K. Renaud, and L. A. Wood, "Teachers' perspectives and practice of cybersecurity education in primary schools," *Discov. Educ.*, vol. 4, no. 1, 2025, doi: 10.1007/s44217-025-00471-0.

Copyright © 2025 by the authors. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited (CC BY 4.0).