Journal of Economics, Entrepreneurship, Management Business and Accounting, 2026, 4(5),577-590.
https://doi.org/10.61255/jeemba.v4i5.1672

Managing cybersecurity vigilance through people, process, and technology: A mixed-methods study

Bondan Widiawan[1*], Ali Muktiyanto[2], Martino Wibowo[3], and Ami Pujiwati[4]

[1] Doctoral Programme of Management Science, Universitas Terbuka, Tangerang Selatan, Indonesia
[2] Faculty of Economics and Business, Universitas Terbuka, Tangerang Selatan, Indonesia
[3] Department of Management, Universitas Terbuka, Tangerang Selatan, Indonesia
[4] Department of Management, Universitas Terbuka, Tangerang Selatan, Indonesia

ABSTRACT

Purpose - This study examines how the People, Process, and Technology (PPT) pillars jointly shape cybersecurity vigilance in Indonesian university settings and whether formal process becomes behaviorally consequential through human capability.
Design/methodology/approach - A quantitatively dominant mixed-methods design combined survey data from 1,684 respondents with interviews involving nine cybersecurity experts. Covariance-based structural equation modeling was conducted in IBM SPSS AMOS, while expert evidence was used for explanatory triangulation.
Finding/Results - People and Technology were significantly associated with vigilance, whereas Process had no significant direct relationship. Process operated indirectly through People (indirect effect = 0.402; Sobel Z = 4.331; $p < .001$). Digital literacy and perceived regulatory reinforcement strengthened selected PPT-vigilance relationships.
Originality/Value - The study reframes PPT as an interdependent organizational governance architecture rather than three competing pillars. It shows that formal process requires human internalization and that technical, behavioral, and regulatory conditions should be managed as an integrated cybersecurity capability.

ARTICLE INFO

Keywords:
cybersecurity vigilance, people-process-technology, cybersecurity governance, digital literacy, structural equation modeling

Article Information:
Received: 14/3/2026
Revised: 20/6/2026
Accepted: 15/8/2026

ISSN:
2985-3168 (Online)
2985-3222 (Print)

***Corresponding Author at:**
Doctoral Programme of Management Science, Universitas Terbuka, Tangerang Selatan, Indonesia.
E-mail address: 530055204@ecampus.ut.ac.id (Bondan Widiawan)

1. Introduction

Cybersecurity is no longer only a technical-control problem; it is an organizational management problem involving human capability, formal process, technology, and governance. As organizations digitize core activities, cybersecurity failures can interrupt service delivery, weaken trust, and increase compliance and recovery costs. Contemporary behavioral cybersecurity research therefore moves beyond the simplistic claim that people are merely the "weakest link" and instead treats secure behavior as a product of capability, motivation, context, and system design (Alsharida et al., 2023; Baltuttis et al., 2024; Chaudhary, 2024). The Global Cybersecurity Index similarly emphasizes that sustainable cyber capacity combines technical, organizational, legal, cooperative, and human-development dimensions (International Telecommunication Union, 2024).

The Indonesian threat environment makes this management challenge especially salient. The National Cyber and Crypto Agency reported 330,527,636 anomalous traffic events during 2024, including 81,286,596 Mirai-botnet activities and 26,771,610 phishing activities; the same landscape recorded 1,367 incident-indication notifications and 241 suspected data-leak incidents identified through cyber-threat-intelligence monitoring (Badan Siber dan Sandi Negara [BSSN], 2025). These categories are not equivalent to confirmed breaches, but they illustrate the scale and diversity of the operating environment in which organizations must manage security behavior and controls.

Indonesia's regulatory environment has also changed materially through Law No. 27 of 2022 on Personal Data Protection (Republic of Indonesia, 2022). Formal regulation strengthens data-governance obligations, yet legal rules do not automatically produce secure day-to-day behavior. Information-security research shows that compliance depends on how rules are interpreted, internalized, and supported by self-efficacy, social influence, perceived consequences, management commitment, and organizational practice (Bulgurcu et al., 2010; Herath & Rao, 2009; Siponen & Vance, 2010). From a management perspective, the central question is therefore not whether policies and technology exist, but how they are translated into recurring vigilance.

The People-Process-Technology (PPT) lens offers an integrative way to examine these dependencies, but it is frequently applied as a descriptive checklist rather than tested as a behavioral architecture. Prior research separately demonstrates that self-efficacy and threat appraisal shape protective action (Johnston & Warkentin, 2010; Ng et al., 2009; Workman et al., 2008), policies and security-management practices shape compliance-related beliefs (Bulgurcu et al., 2010; Vance et al., 2012), and technical safeguards require appropriate human use. Less is known about how these elements operate together when the outcome is recurring cybersecurity vigilance and when digital literacy and perceived regulatory reinforcement alter the strength of key relationships.

Accordingly, this study investigates cybersecurity vigilance among 1,684 respondents drawn from multiple Indonesian university settings, supplemented by interviews with nine cybersecurity experts. The unit of analysis in the quantitative strand is the individual respondent within the sampled university networks. The study asks whether People, Process, and Technology are associated with vigilance; whether People mediates the Process-Vigilance relationship; and whether digital literacy and regulatory reinforcement moderate selected PPT pathways. By shifting attention from ranking isolated pillars to explaining their

interdependence, the study contributes an organizational governance model that is directly relevant to cybersecurity capability management.

2. Literature Review & Hypothesis Development

2.1. Theoretical foundation

Social Cognitive Theory (SCT) provides the principal behavioral foundation of the model. SCT explains behavior through reciprocal interaction among personal cognition, behavior, and environmental conditions, with self-efficacy representing a central mechanism through which individuals judge whether they can perform a required action (Bandura, 1997; Compeau & Higgins, 1995). In cybersecurity, self-efficacy matters because users must not only know that a threat exists but also believe that they can recognize, avoid, report, or remediate it. The People pillar is therefore represented by self-efficacy and risk perception rather than by a broad undifferentiated notion of "human error."

Protection Motivation Theory (PMT) complements SCT by explaining why perceived threats become protective action. PMT distinguishes threat appraisal from coping appraisal; behavior is more likely when individuals perceive meaningful risk and believe that an effective response is available and within their capability (Rogers, 1983). Cybersecurity research repeatedly applies this logic to phishing, security-policy compliance, and protective computing practices (Boss et al., 2015; Johnston & Warkentin, 2010; Ng et al., 2009). In the present study, PMT helps explain why risk perception and self-efficacy jointly form a proximal behavioral mechanism linking organizational conditions to vigilance.

The Process pathway is interpreted through the knowledge-creation view of organizations. Formal policies, standard operating procedures, audits, and incident-reporting rules constitute explicit organizational knowledge; they become behaviorally meaningful only when individuals understand, internalize, and enact them in recurring practice (Nonaka & Toyama, 2003). This perspective provides the rationale for modeling People as a mediator between Process and vigilance: process may be necessary, but its effect depends on whether formal rules are converted into usable individual capability.

Digital literacy and regulatory reinforcement are modeled as contextual conditions rather than additional PPT pillars. Digital literacy can strengthen users' capacity to interpret threat information, distinguish credible from deceptive content, and use security controls correctly, whereas perceived regulation can increase the salience of security obligations and consequences. Deterrence-oriented security research supports the view that regulatory and sanction-related signals influence compliance when they are translated into organizational expectations (Herath & Rao, 2009; Siponen & Vance, 2010). Together, SCT, PMT, knowledge conversion, and regulatory reinforcement explain why PPT relationships may be direct, indirect, and contingent rather than uniformly additive.

2.2. Empirical evidence and research gap

Empirical research on the People pillar consistently shows that security behavior varies with efficacy, threat beliefs, attitudes, awareness, and user profiles. The Human Aspects of Information Security Questionnaire tradition demonstrates that information-security awareness is multidimensional (Parsons et al., 2014), while comparative evidence shows that cybersecurity knowledge does not necessarily translate into safe behavior (Zwilling et al., 2022). More recent work similarly identifies heterogeneous behavioral patterns among knowledge workers and non-IT employees, reinforcing the need to model human capability

within its technical and organizational context rather than treating it as a single deficit variable (Baltuttis et al., 2024; Fatoki et al., 2024).

Process-oriented studies show that security policies and sanctions can influence compliance, but their effects depend on beliefs, norms, habits, and perceived organizational commitment (Bulgurcu et al., 2010; Herath & Rao, 2009; Vance et al., 2012). Technology, by contrast, provides structural safeguards and affordances that can reduce exposure and support secure action, yet its effectiveness remains intertwined with correct use and user decision-making (Workman et al., 2008). Cybersecurity-culture research further emphasizes that management support, communication, and routine practice are necessary for policies and controls to become sustainable behavior (Alshaikh, 2020).

Digital literacy and regulation address two additional contextual gaps. Awareness and knowledge are related to security behavior but do not map perfectly onto it (Parsons et al., 2014; Zwilling et al., 2022), suggesting that literacy may strengthen some behavioral and technical pathways without necessarily improving policy adherence. Recent training research also argues that cybersecurity interventions should be evaluated by behavioral outcomes rather than knowledge acquisition alone (Chaudhary, 2024; Prümmer et al., 2024). The remaining gap is therefore mechanistic: how are PPT components connected, and under what contextual conditions do their relationships with vigilance become stronger or weaker?

Table 1 synthesizes this gap and positions the study within behavioral and organizational cybersecurity research.

Table 1. Research gap and contribution of the present study

Research issue	Prior evidence and unresolved issue	Contribution of this study
Human capability	Self-efficacy, threat appraisal, awareness, and attitudes predict secure behavior, but users remain heterogeneous (Johnston & Warkentin, 2010; Alsharida et al., 2023).	Models People as a proximal behavioral mechanism inside a broader PPT architecture.
Security process	Policies and sanctions can shape compliance, but effects depend on awareness, efficacy, norms, and internalization (Bulgurcu et al., 2010; Herath & Rao, 2009).	Tests both the Process-Vigilance path and the mediated Process-People-Vigilance path.
Technology	Technical controls are necessary, while user behavior remains consequential to their effective use (Workman et al., 2008; Fatoki et al., 2024).	Tests Technology as a direct predictor when People and Process are modeled simultaneously.
Knowledge-behavior gap	Awareness and knowledge do not consistently translate into protective action (Parsons et al., 2014; Zwilling et al., 2022).	Tests Digital Literacy as a moderator of selected PPT-Vigilance relationships.
Regulatory context	Security behavior reflects organizational and deterrence-related conditions (Herath & Rao, 2009; Siponen & Vance, 2010).	Tests perceived regulatory reinforcement as a moderator of People and Process relationships.

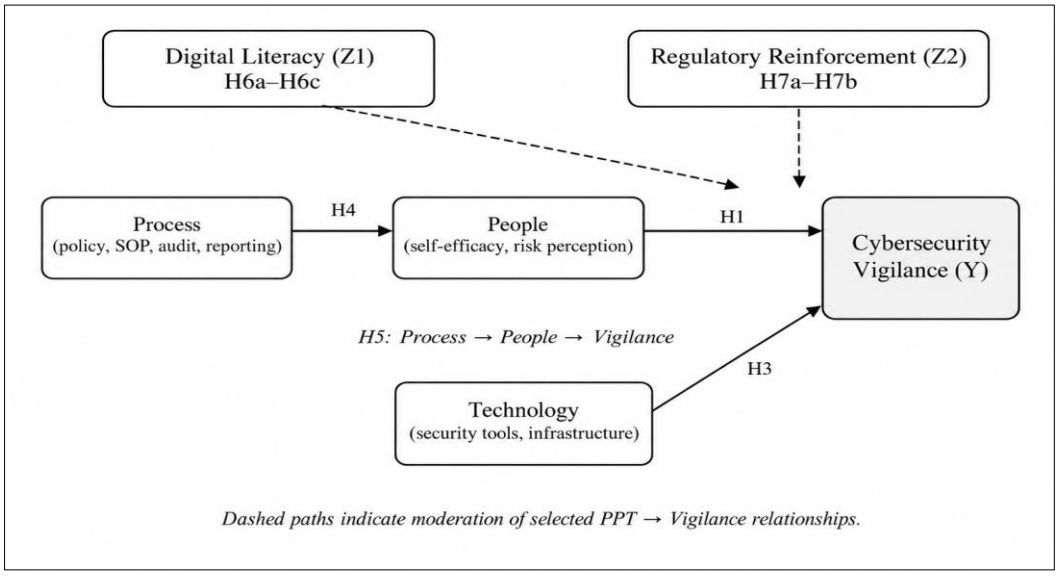
Source: Authors' synthesis from the cited literature.

The novelty lies in modeling direct PPT relationships, Process-People mediation, and contextual moderation within a single governance architecture. This avoids treating statistical significance as evidence that one pillar is inherently "dominant" and instead focuses on the pathways through which vigilance is produced.

2.3. Hypotheses and conceptual model

H1. People (self-efficacy and risk perception) is positively associated with cybersecurity vigilance.

H2. Process is positively associated with cybersecurity vigilance.
H3. Technology is positively associated with cybersecurity vigilance.
H4. Process is positively associated with People.
H5. People mediates the relationship between Process and cybersecurity vigilance.
H6a. Digital literacy positively moderates the People-Vigilance relationship.
H6b. Digital literacy positively moderates the Process-Vigilance relationship.
H6c. Digital literacy positively moderates the Technology-Vigilance relationship.
H7a. Perceived regulatory reinforcement positively moderates the People-Vigilance relationship.
H7b. Perceived regulatory reinforcement positively moderates the Process-Vigilance relationship.
Figure 1 integrates these hypotheses into a single model in which cybersecurity vigilance is the dependent construct, People operates as both a direct predictor and mediator, and Digital Literacy and Regulatory Reinforcement moderate selected PPT-Vigilance relationships.



Source: Authors' conceptualization.

Figure 1. Hypothesized People-Process-Technology model of cybersecurity vigilance

The model treats the PPT pillars as interdependent. Process can relate to vigilance directly and indirectly through People; Technology and People can relate to vigilance directly; and the two contextual moderators condition selected relationships. This specification provides the basis for the empirical tests.

3. Methodology

3.1. Research design and setting

The study used a quantitatively dominant mixed-methods design combining a survey/structural-equation-modeling strand with a qualitative expert-interview strand. Integration occurred during interpretation, where expert evidence was used to contextualize the structural relationships and generate organizational implications (Creswell & Plano Clark, 2018; Fetters et al., 2013). The study was conducted from June 2025 to February 2026 across Indonesian university settings, with expert participation from academia, government, and industry.

3.2. Sampling and participants

The quantitative dataset comprised 1,684 respondents associated with multiple university settings in Indonesia. Educational backgrounds ranged from senior high school/vocational education to doctoral level. The sampling frame was institution-based and was not designed for probability-based national inference; accordingly, the results are interpreted within the sampled university networks rather than as population-representative estimates for Indonesia. The qualitative strand involved nine cybersecurity experts drawn from academia, the National Cyber and Crypto Agency (BSSN), and industry. The individual respondent is the unit of analysis in the quantitative strand.

3.3. Measures

Survey items used five-point Likert response options (1 = strongly disagree to 5 = strongly agree). In the estimated measurement model, People was represented by self-efficacy and risk perception; Process by formal policy and security-process indicators; Technology by security-control and infrastructure indicators; and Cybersecurity Vigilance by precautionary, reporting, and responsibility-related behaviors. Digital Literacy and Regulatory Reinforcement were treated as observed composite moderators. Table 2 summarizes the operationalization used in the analysis.

Table 2. Operationalization of study variables

Construct	Operational indicators used in the analysis	Analytical role
People (X1)	Self-efficacy; risk perception.	Latent PPT pillar; direct predictor and mediator.
Process (X2)	Documented cybersecurity policy; SOP compliance; periodic security audits; incident reporting; compliance procedures. The study instrument includes one regulation-linked compliance item.	Latent PPT pillar; direct predictor and antecedent of People.
Technology (X3)	Firewall/antivirus availability; layered security technology; regular system updates; effective MFA use; AI-based threat-detection implementation.	Latent PPT pillar; direct predictor.
Digital Literacy (Z1)	Understanding basic cybersecurity terminology; keeping current with cybersecurity trends; distinguishing credible from false information.	Observed composite moderator of selected PPT-Vigilance paths.
Regulatory Reinforcement (Z2)	Perceived discipline induced by the Personal Data Protection Law; perceived sanction pressure; perceived external reinforcement of internal security policy.	Observed composite moderator of People/Process-Vigilance paths.
Cybersecurity Vigilance (Y)	Checks before clicking links; password-management practice; immediate reporting of suspicious activity; personal responsibility for data security; vigilance as an organizational/professional responsibility.	Latent outcome construct.

Source: Authors' operationalization based on the study instrument.

Several Process and Technology indicators refer to organizational capabilities but were reported by individuals. Interpretation therefore focuses on perceived institutional conditions and individual vigilance rather than objective control maturity. The regulation-linked Process item is also acknowledged as a potential source of conceptual overlap with the separate Regulatory Reinforcement moderator.

3.4. Data analysis and mixed-method integration

The quantitative strand used covariance-based structural equation modeling (CB-SEM) in IBM SPSS AMOS. The measurement model was evaluated using standardized loading factors

(SLF), average variance extracted (AVE), and composite reliability (CR). Values above .50 for AVE and above .70 for CR were treated as evidence of acceptable convergent validity and reliability (Fornell & Larcker, 1981). Structural-model fit was evaluated from the reported RMR, RMSEA, GFI, NFI, RFI, IFI, TLI, CFI, and AGFI values, interpreted jointly rather than through a single index (Hu & Bentler, 1999).

Direct and moderation hypotheses were evaluated from the p-values reported in the structural output. Because a complete set of standardized structural coefficients was not available for every structural path, the analysis does not use the reported path statistics to rank substantive effect magnitude. Mediation was evaluated from the Process-People (a) and People-Vigilance (b) paths and their standard errors. The indirect effect was calculated as a × b and evaluated with the Sobel statistic; a significant indirect effect combined with a nonsignificant direct Process-Vigilance path is interpreted as indirect-only mediation (Zhao et al., 2010).

The expert-interview material was used for explanatory triangulation rather than for prevalence estimation. Recurring expert judgments were compared with the quantitative pattern to identify convergence concerning legal foundations, human capability, and cross-sector coordination. The qualitative strand was therefore interpreted as contextual evidence, and no claims are made about theme prevalence or statistical generalization from the expert sample.

4. Result and Discussion

4.1. Measurement and structural model results

The measurement model was first assessed through standardized loading factors, AVE, and composite reliability. Table 3 consolidates the indicator loadings and construct-level validity and reliability evidence.

Table 3. Measurement model: standardized loadings, AVE, and composite reliability

Construct	Indicator	SLF	AVE	CR
People	Self-efficacy	.864	.74	.85
People	Risk perception	.858		
Process	Pr1	.848	.72	.93
Process	Pr2	.867		
Process	Pr3	.842		
Process	Pr4	.869		
Process	Pr5	.819		
Technology	Te1	.799	.69	.92
Technology	Te2	.837		
Technology	Te3	.841		
Technology	Te4	.844		
Technology	Te5	.823		
Cybersecurity Vigilance	Ks1	.802	.69	.92
Cybersecurity Vigilance	Ks2	.801		
Cybersecurity Vigilance	Ks3	.836		
Cybersecurity Vigilance	Ks4	.861		
Cybersecurity Vigilance	Ks5	.855		

Notes: AVE > .50 and CR > .70 were treated as acceptable. Blank AVE/CR cells indicate that the construct-level value is reported once at the first indicator.

Source: Authors' analysis of study data.

All reported loadings exceeded .79, AVE ranged from .69 to .74, and CR ranged from .85 to .93. These results support convergent validity and internal consistency for the four latent

constructs represented in the reported measurement model. Digital Literacy and Regulatory Reinforcement were modeled as observed composites and are therefore not included in the latent AVE/CR assessment.

Structural-model fit was then examined using the set of indices shown in Table 4. The evidence is interpreted as a pattern rather than selectively emphasizing only favorable indices.

Table 4. Structural-model fit indices

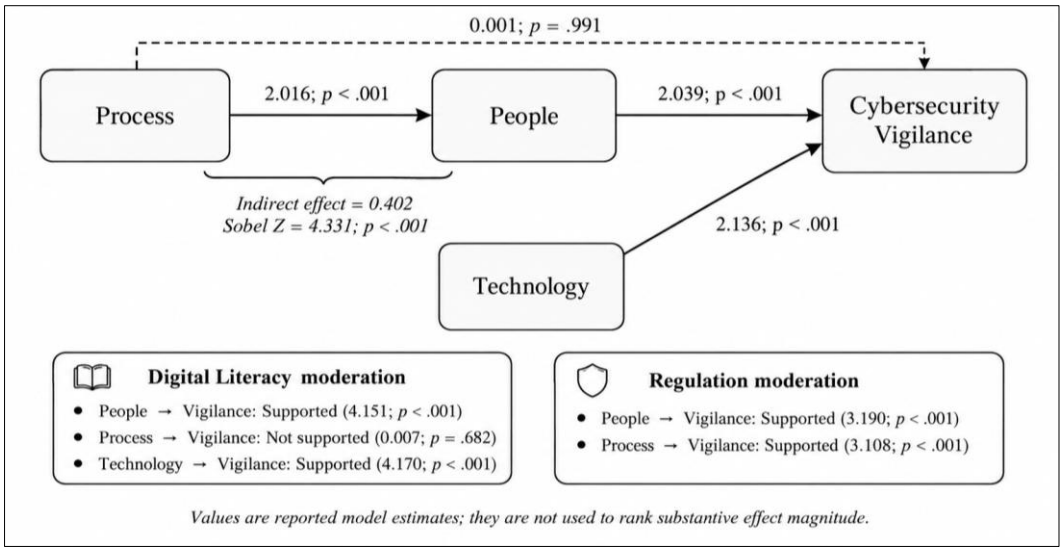
Index	Reported value	Reference benchmark	Interpretation
RMR	.083	≤ .05 (strict benchmark)	Weak/marginal
RMSEA	.079	≤ .08	Acceptable
GFI	.816	≥ .90	Below benchmark
NFI	.980	≥ .90	Good
RFI	.860	≥ .90	Below benchmark
IFI	.931	≥ .90	Good
TLI	.841	≥ .90	Below benchmark
CFI	.930	≥ .90	Good
AGFI	.773	≥ .90	Below benchmark

Source: Authors' analysis of the reported AMOS fit indices.

RMSEA, NFI, IFI, and CFI support an acceptable structural representation, whereas RMR, GFI, RFI, TLI, and AGFI remain below conventional benchmarks. The model is therefore treated as substantively informative but not as evidence of uniformly strong global fit; refinement and independent replication remain warranted.

4.2. Hypothesis, mediation, and moderation results

Figure 2 summarizes the direct and mediated relationships using the reported significance decisions and the calculated indirect effect. To avoid implying effect-size rankings from nonstandardized path statistics, the figure emphasizes the reported significance levels and the calculated indirect effect.



Source: Authors' analysis of the reported structural output.

Figure 2. Direct and mediated structural relationships

People and Technology show significant direct relationships with Cybersecurity Vigilance, whereas the direct Process-Vigilance relationship is not significant. Process is significantly related to People, and the indirect Process-People-Vigilance relationship is significant. Table 5 adds the moderation results and formal hypothesis decisions.

Table 5. Hypothesis testing, mediation, and moderation results

Hypothesis	Relationship/test	Reported significance / effect	Decision
H1	People → Cybersecurity Vigilance	$p < .001$	Supported
H2	Process → Cybersecurity Vigilance	$p = .991$	Not supported
H3	Technology → Cybersecurity Vigilance	$p < .001$	Supported
H4	Process → People	$p < .001$	Supported
H5	Process → People → Vigilance	Indirect effect = .402; Sobel $Z = 4.331$; $p < .001$	Indirect-only mediation
H6a	People × Digital Literacy → Vigilance	$p < .001$	Supported
H6b	Process × Digital Literacy → Vigilance	$p = .682$	Not supported
H6c	Technology × Digital Literacy → Vigilance	$p < .001$	Supported
H7a	People × Regulation → Vigilance	$p < .001$	Supported
H7b	Process × Regulation → Vigilance	$p < .001$	Supported

Notes: For H5, $a = .916$ (SE = .202) and $b = .439$ (SE = .030), yielding $.916 \times .439 = .402$. Direct and moderation decisions use the p-values reported in the structural output.

Source: Authors' analysis and mediation calculation.

The results support H1, H3, H4, H6a, H6c, H7a, and H7b; H2 and H6b are not supported. The mediation result indicates that formal Process is related to vigilance through the People mechanism rather than through an independently significant direct path. These decisions concern statistical support for the specified relationships and should not be interpreted as a ranking of PPT pillars by effect magnitude.

4.3. Mixed-method integration

The expert-interview strand was used to contextualize the quantitative architecture. Table 6 presents a joint display linking the structural pattern to expert-informed interpretations and managerial implications.

Table 6. Joint display integrating quantitative findings and expert interpretation

Quantitative result	Expert-informed interpretation	Managerial implication
People and Technology show significant direct relationships with Vigilance.	Experts emphasized the human element as a decisive operational point even when technical controls are present.	Treat users as active security actors and pair technical investments with capability-building and usable security practices.
Process has no significant direct path, but Process-People and the indirect Process-People-Vigilance pathway are significant.	Experts emphasized moving beyond formal compliance toward internalized security habits and culture.	Translate policy and SOPs into repeated practice, role-specific guidance, incident exercises, and feedback loops.
Digital Literacy moderates People and Technology paths, but not the Process path.	Experts stressed practical interpretation of threats rather than document awareness alone.	Use literacy interventions to improve threat interpretation and effective tool use; do not assume literacy alone creates policy compliance.
Regulatory reinforcement moderates People and Process paths.	Experts emphasized stronger legal foundations and salient data-protection responsibilities.	Connect regulatory obligations to procedures, communication, accountability, and routine decision points.
PPT effects are interdependent rather than independently dominant.	Experts emphasized collaboration among government, academia, and industry.	Develop people capability, process design, and technology as one coordinated socio-technical system.

Source: Authors' mixed-method integration.

The joint display shows convergence on a human-centric but not human-exclusive interpretation. Human capability is central because it mediates the translation of Process into vigilance, Technology retains a direct structural role, and contextual conditions alter the strength of several relationships.

4.4. Discussion

The central contribution of the study is a shift from ranking PPT pillars to explaining their architecture. People and Technology are directly associated with cybersecurity vigilance, whereas Process does not exhibit a significant direct relationship. Yet Process remains consequential because it predicts People and the Process-People-Vigilance indirect effect is significant. Because dominance cannot be inferred from significance tests alone, the more defensible interpretation is that human capability is a proximal mechanism through which formal process becomes behaviorally consequential.

The People result is consistent with SCT and PMT. Self-efficacy helps explain whether users believe they can perform protective actions, while risk perception makes threats salient enough to motivate attention and precaution (Bandura, 1997; Rogers, 1983). Cybersecurity studies repeatedly find that efficacy and threat-related beliefs influence protective intentions and behaviors, although their strength depends on context and task (Boss et al., 2015; Johnston & Warkentin, 2010; Workman et al., 2008). Amin et al. (2025) likewise reinforces the continuing relevance of self-efficacy for cybersecurity behavior among IT employees. In management terms, the People pillar should therefore be treated as an organizational capability that can be developed, supported, and embedded in work routines.

Technology also shows a significant direct relationship with vigilance. This is important because a strongly human-centric argument becomes misleading if it implies that secure behavior can compensate for inadequate controls. Security technologies alter the choice environment: multi-factor authentication, endpoint protection, updates, and detection capabilities can make secure action easier, reduce exposure to individual mistakes, and provide cues that support vigilance. At the same time, technology remains dependent on comprehension and correct use. Evidence on user typologies and non-IT employees supports this interaction between personal dispositions and technical context (Baltuttis et al., 2024; Fatoki et al., 2024).

The Process finding deserves particular attention. A nonsignificant direct Process-Vigilance relationship does not demonstrate that policy and SOPs are unimportant; the significant indirect pathway instead suggests that process must be internalized through human cognition and practice before it is reflected in vigilance. This interpretation aligns with knowledge-creation theory, in which explicit knowledge becomes operational when it is internalized and enacted (Nonaka & Toyama, 2003), and with security-compliance research showing that policy effects depend on awareness, self-efficacy, normative beliefs, habit, and perceived consequences (Bulgurcu et al., 2010; Herath & Rao, 2009; Vance et al., 2012). The practical implication is not "less process," but process designed for behavioral uptake.

Digital Literacy strengthens the People-Vigilance and Technology-Vigilance relationships but not the Process-Vigilance relationship. This pattern is coherent if literacy is understood as a cognitive-technical capability: it can help users recognize suspicious information, interpret warnings, and use security tools effectively, thereby making self-efficacy operational rather than merely perceptual. It does not automatically create policy adherence when compliance depends on incentives, workflow, role clarity, and enforcement. The result is consistent with the documented knowledge-behavior gap (Parsons et al., 2014; Zwilling et al., 2022) and with arguments that security education should be assessed by behavior change rather than knowledge acquisition alone (Chaudhary, 2024; Prümmer et al., 2024).

The nonsignificant Digital Literacy × Process interaction also cautions managers against treating every cybersecurity deficit as a training problem. If process requirements are poorly aligned with work routines, overly complex, weakly enforced, or perceived as irrelevant, additional literacy may not strengthen the process-behavior relationship. This observation accords with cybersecurity-culture research emphasizing management support, local norms, communication, and practice design rather than information transmission alone (Alshaikh, 2020). Future models should therefore examine policy usability, security climate, and implementation quality as mechanisms linking formal process to individual vigilance.

Perceived Regulatory Reinforcement strengthens both the People-Vigilance and Process-Vigilance relationships. The result should not be interpreted as evidence that the Personal Data Protection Law directly causes vigilance because the design is cross-sectional and the moderator captures perceived reinforcement rather than objective enforcement. Nevertheless, the pattern is compatible with deterrence and policy-compliance research: formal obligations become behaviorally meaningful when users perceive consequences, organizational commitment, and implementation support (Herath & Rao, 2009; Siponen & Vance, 2010). For organizational governance, this means regulatory compliance should be translated into role clarity, procedures, managerial accountability, and routine decision points.

From a management perspective, the findings support an integrated resource-allocation logic. Policies, training, and technical controls should not be managed as separate workstreams because their value depends on how they reinforce one another. Human capability is central not because it is proven to have the largest standardized effect - such evidence is unavailable - but because it occupies multiple structural roles: a direct predictor, a mediator of Process, and a pathway conditioned by literacy and regulation. This architecture provides a more useful basis for cybersecurity governance than a simple pillar ranking and offers a testable foundation for future multilevel and longitudinal research.

5. Conclusion and Suggestion

This study develops an organizational, human-centric but socio-technical account of cybersecurity vigilance using the People-Process-Technology framework. Within the sampled Indonesian university networks, People and Technology are directly associated with vigilance, while Process becomes behaviorally consequential primarily through People. Digital Literacy strengthens the People and Technology pathways, whereas perceived Regulatory Reinforcement strengthens the People and Process pathways. The contribution is therefore not a ranking of isolated pillars, but a pathway model in which human capability translates formal process into practice, technology provides structural support, and contextual literacy and regulation condition key relationships.

For managers and institutional leaders, cybersecurity policy, workforce capability, and technology investment should be governed as an integrated portfolio. Policies should be actionable and rehearsed; users should receive role-specific support that develops self-efficacy and threat interpretation; technical controls should facilitate rather than obstruct secure action; and data-protection obligations should be translated into visible organizational responsibilities. The potential managerial and economic benefit is better allocation of security resources by reducing isolated investments that do not translate into behavior. Future decision-making should therefore prioritize complementarity among people, process, and technology rather than assuming that expenditure on any single pillar is sufficient.

6. Limitations and Future Research

Several limitations qualify interpretation. First, the quantitative strand is cross-sectional and self-reported, so relationships are associational and may be affected by common-method variance (Podsakoff et al., 2003). Second, respondents came from university settings and should not be treated as representative of the Indonesian population or all business sectors. Third, the institution-based sampling frame limits population inference, and several Process and Technology indicators describe organizational capabilities but were assessed through individuals. Fourth, one Process indicator is regulation-linked, creating potential conceptual overlap with the Regulatory Reinforcement moderator. Fifth, the two moderator composites were not reported with the same latent psychometric detail as the PPT constructs, and the global fit evidence is mixed. Finally, the expert-interview strand was designed for explanatory triangulation rather than a standalone prevalence-oriented qualitative analysis, which limits claims about saturation and theme frequency.

Future research should test the architecture longitudinally and across sectors such as banking, public administration, higher education, and digital services. Replications should use probability or clearly documented purposive sampling where feasible, multilevel designs that separate organizational controls from individual perceptions, behavioral logs or incident records, standardized structural coefficients with bootstrapped confidence intervals, and fuller validation of moderator constructs. Qualitative extensions should report interview protocols, coding procedures, saturation criteria, and negative cases so that the integration of quantitative and qualitative evidence is fully auditable.

Acknowledgement

The authors acknowledge the respondents and cybersecurity experts whose participation informed the study.

Declaration of AI and AI-assisted technologies in the writing process

During the preparation of this manuscript, the authors used ChatGPT (OpenAI) to support language editing, structural organization, and presentation refinement. The authors reviewed and edited the resulting text and figures as needed and take full responsibility for the content of the publication.

Reference

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, *98*, 102003. doi:10.1016/j.cose.2020.102003

Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society*, *73*, 102258. doi:10.1016/j.techsoc.2023.102258

Amin, M. A. S., Prybutok, V., & Rishat, M. A. S. A. (2025). The role of self-efficacy in IT employee cybersecurity safety behavior. *International Journal of Human–Computer Interaction*. Advance online publication. doi:10.1080/10447318.2025.2607558

Badan Siber dan Sandi Negara. (2025). *Lanskap Keamanan Siber Indonesia 2024 [Indonesia cybersecurity landscape 2024].* Retrieved from https://www.bssn.go.id/

Baltuttis, D., Teubner, T., & Adam, M. T. P. (2024). A typology of cybersecurity behavior among knowledge workers. *Computers & Security*, *140*, 103741. doi:10.1016/j.cose.2024.103741

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

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 security behaviors. *MIS Quarterly*, *39*(4), 837–864. doi:10.25300/MISQ/2015/39.4.5

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548. doi:10.2307/25750690

Chaudhary, S. (2024). Driving behaviour change with cybersecurity awareness. *Computers & Security*, *142*, 103858. doi:10.1016/j.cose.2024.103858

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, *19*(2), 189–211. doi:10.2307/249688

Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3rd ed.). SAGE.

Fatoki, J. G., Shen, Z., & Mora-Monge, C. A. (2024). Optimism amid risk: How non-IT employees' beliefs affect cybersecurity behavior. *Computers & Security*, *141*, 103812. doi:10.1016/j.cose.2024.103812

Fetters, M. D., Curry, L. A., & Creswell, J. W. (2013). Achieving integration in mixed methods designs—Principles and practices. *Health Services Research*, *48*(6 Pt 2), 2134–2156. doi:10.1111/1475-6773.12117

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39–50. doi:10.1177/002224378101800104

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. doi:10.1057/ejis.2009.6

Hu, L.-t., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal*, *6*(1), 1–55. doi:10.1080/10705519909540118

International Telecommunication Union. (2024). *Global Cybersecurity Index 2024* (5th ed.). Retrieved from https://www.itu.int/pub/D-HDB-GCI.01-2024

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549–566. doi:10.2307/25750691

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815–825. doi:10.1016/j.dss.2008.11.010

Nonaka, I., & Toyama, R. (2003). The knowledge-creating theory revisited: Knowledge creation as a synthesizing process. *Knowledge Management Research & Practice*, *1*(1), 2–10. doi:10.1057/palgrave.kmrp.8500001

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, *42*, 165–176. doi:10.1016/j.cose.2013.12.003

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879–903. doi:10.1037/0021-9010.88.5.879

Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security*, *136*, 103585. doi:10.1016/j.cose.2023.103585

Republic of Indonesia. (2022). *Law of the Republic of Indonesia Number 27 of 2022 concerning Personal Data Protection.* Retrieved from https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo & R. Petty (Eds.), *Social psychophysiology* (pp. 153-176). Guilford Press.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487–502. doi:10.2307/25750688

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and Protection Motivation Theory. *Information & Management*, *49*(3–4), 190–198. doi:10.1016/j.im.2012.04.002

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799–2816. doi:10.1016/j.chb.2008.04.005

Zhao, X., Lynch, J. G., Jr., & Chen, Q. (2010). Reconsidering Baron and Kenny: Myths and truths about mediation analysis. *Journal of Consumer Research*, *37*(2), 197–206. doi:10.1086/651257

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82–97. doi:10.1080/08874417.2020.1712269