Research Article

R.A.N. Vol. 13 (1) 2027
ran.udec.cl

RAN
REVISTA ACADEMIA & NEGOCIOS

When Risk Awareness Is Not Enough: The Role of Threat Perception in Cybersecurity Behavior among Digital Executives

CUANDO LA CONCIENCIA DEL RIESGO NO ES SUFICIENTE: EL PAPEL DE LA PERCEPCIÓN DE AMENAZAS EN EL COMPORTAMIENTO DE CIBERSEGURIDAD ENTRE EJECUTIVOS DIGITALES

Freddy Alvarado-Vargas[1*]
Universidad de Lima

Diego Norena-Chavez[1]
Universidad de Lima

* Corresponsal author.

1 Escuela de Postgrado de la Universidad de Lima, Avenida Javier Prado Este 4600, distrito de Santiago de Surco provincia y departamento de Lima, 15023, PERÚ.

Abstract

Purpose: Increasing cyber incidents show that organizational security depends not only on technology but also on human decision-making. However, prior behavioral cybersecurity research provides limited evidence on how technically experienced professionals translate cyber risk awareness into protective action. Drawing on the Technology Threat Avoidance Theory (TTAT) and the Behavioral Cybersecurity Framework (BCF), this study identifies the cognitive determinants of Cybersecurity Behavior (CSB) and examines the mediating role of Threat Perception (TP).

Methodology: A quantitative, cross-sectional, post-positivist study analyzed six constructs using Partial Least Squares Structural Equation Modeling (PLS-SEM). Data were collected through non-probabilistic sampling from 311 digital executives in Lima, Peru. Importance–Performance Map Analysis (IPMA) identified managerial priorities.

Results:
TP directly influenced CSB ($\beta = 0.305$, $p = 0.002$) and significantly mediated the effect of Severity Perception (SP) ($\beta = 0.165$, $p = 0.006$). Privacy Concern (PC) and Risk Perception (RP) were non-significant. The model explained 15.0% of CSB variance ($R^2 = 0.150$), while IPMA identified Response Costs (RC) as the main managerial improvement opportunity.

Implications: Cybersecurity interventions should strengthen the perceived relevance of cyber threats while reducing operational barriers, extending TTAT by showing that severity awareness alone does not activate protective behavior among technically experienced executives.

Originality: Using evidence from digital executives in an emerging economy, this study shows that technical expertise alone does not ensure secure behavior. Threat Perception bridges the gap between risk awareness and protective action, extending behavioral cybersecurity theory in expert decision-making contexts.

ARTICLE INFO
Received: 10 December 2025
Accepted: 2 June 2026

Keywords:
Cybersecurity behavior
Threat perception
Digital executives
Cognition–action gap
Technology Threat Avoidance Theory

ISSN: 0719-7713 / 0719-6245
https://doi.org/10.29393/RAN13-2RNRP20002

Resumen

Propósito: El aumento de los ciberincidentes evidencia que la seguridad organizacional depende no solo de la tecnología, sino también de las decisiones humanas. Sin embargo, existe evidencia limitada sobre cómo los profesionales con alta experiencia técnica transforman la conciencia del riesgo en conductas protectoras. Basado en la Technology Threat Avoidance Theory (TTAT) y el Behavioral Cybersecurity Framework (BCF), este estudio identifica los determinantes cognitivos del Comportamiento de Ciberseguridad (CSB) y analiza el papel mediador de la Percepción de Amenaza (TP).

Metodología: Se realizó un estudio cuantitativo, transversal y postpositivista mediante Modelado de Ecuaciones Estructurales por Mínimos Cuadrados Parciales (PLS-SEM) con una muestra no probabilística de 311 ejecutivos digitales de Lima, Perú. Además, se aplicó un Análisis de Mapa de Importancia–Desempeño (IPMA) para establecer prioridades de gestión.

Resultados: La Percepción de Amenaza influyó significativamente en el CSB ($\beta = 0.305$; $p = 0.002$) y medió la relación entre la Percepción de Severidad y el comportamiento protector ($\beta = 0.165$; $p = 0.006$). La Preocupación por la Privacidad y la Percepción del Riesgo no mostraron efectos significativos. El modelo explicó el 15.0 % de la varianza del CSB ($R^2 = 0.150$), mientras que el IPMA identificó los Costos de Respuesta como la principal oportunidad de mejora.

Implicaciones: Los programas de ciberseguridad deben fortalecer la relevancia percibida de las amenazas y reducir las barreras operativas, ampliando la TTAT al demostrar que la conciencia de la severidad, por sí sola, no activa conductas protectoras en ejecutivos con alta experiencia técnica.

Originalidad: A partir de evidencia obtenida en ejecutivos digitales de una economía emergente, el estudio demuestra que la experiencia técnica no garantiza un comportamiento seguro. La Percepción de Amenaza constituye el mecanismo cognitivo que transforma la conciencia del riesgo en conductas protectoras y amplía la comprensión de la ciberseguridad conductual en contextos de decisión especializada.

INFORMACIÓN ARTÍCULO
Recibido: 10 de Diciembre 2025
Aceptado: 2 de Junio 2026

Keywords:
Comportamiento de ciberseguridad
Percepción de amenaza
Ejecutivos digitales
Brecha cognición–acción
Teoría de la Evitación de Amenazas Tecnológicas

INTRODUCTION

The rapid escalation of social engineering threats and the malicious use of artificial intelligence have placed users (particularly digital executives) at the center of organizational cybersecurity resilience.

In this study, digital executives are defined as senior professionals whose managerial responsibilities include decision-making concerning digital infrastructure, technology governance, and cybersecurity risk management within their organizations. Unlike operational employees, whose cybersecurity behavior is typically associated with compliance with established policies, digital executives participate in strategic decisions such as evaluating technological risks, prioritizing cybersecurity investments, approving protection protocols, and allocating resources for digital security. Consequently, their behavior extends beyond individual practices and may influence the resilience of the organization's digital ecosystem. Understanding how this group perceives technological risks and responds through protective behavior is therefore critical for strengthening cybersecurity governance.

A significant share of cyber incidents continues to be associated with human error and inadequate risk-management decisions, highlighting the importance of understanding the behavioral determinants of cybersecurity practices. Recent evidence identifies the human factor as one of the most vulnerable elements in organizational cybersecurity (Bishop et al., 2025). Promoting secure behavior therefore

requires strengthening threat perception while reducing barriers to protective action, particularly among digital executives, who are increasingly targeted by sophisticated cyberattacks (Vrhovec & Markelj, 2024).

This context is particularly relevant in emerging economies such as Peru, where rapid digital transformation has expanded organizational dependence on digital technologies while cybersecurity governance capabilities are still evolving. Organizations increasingly face sophisticated cyber threats in environments characterized by heterogeneous levels of cybersecurity maturity, uneven adoption of security practices, and evolving regulatory frameworks. Consequently, understanding how digital executives interpret and respond to cyber risks is especially important for strengthening organizational resilience and supporting secure digital transformation initiatives across Latin America.

Despite growing interest in behavioral cybersecurity, important theoretical questions remain regarding how technically experienced professionals translate cyber risk awareness into protective behavior. Although prior studies have examined multiple perceptual and behavioral determinants, they typically analyze these constructs in isolation or assume that greater risk awareness leads directly to stronger protective responses (Al-Emran et al., 2024; Alrawhani et al., 2025; Arachchilage et al., 2016;). Consequently, little is known about how technical expertise and executive responsibilities influence the cognitive process through which severity awareness becomes protective behavior.

This limitation reflects a potential cognition–action gap: technically experienced professionals may recognize severe cyber risks without consistently adopting secure behavior. Understanding this mechanism is essential for refining behavioral cybersecurity theory and designing more effective organizational interventions. Accordingly, this study examines whether Threat Perception mediates the relationship between Severity Perception and Cybersecurity Behavior among digital executives.

Addressing this theoretical gap, this study examines the cognitive mechanisms underlying cybersecurity behavior among highly specialized digital executives using Technology Threat Avoidance Theory (TTAT) and the Behavioral Cybersecurity Framework (BCF). It contributes by: (1) extending TTAT to explain how Threat Perception transforms severity awareness into protective behavior among expert users; (2) providing evidence from digital executives in Peru, an underexplored Latin American context; and (3) identifying practical priorities that help organizational leaders and CISOs strengthen cybersecurity behavior by increasing threat salience while reducing operational friction.

More specifically, the study explains why technically experienced professionals may recognize severe cyber risks without consistently translating such awareness into protective behavior. The findings show that Severity Perception influences cybersecurity behavior only indirectly through Threat Perception, indicating that awareness of potential damage is insufficient unless threats are interpreted as personally relevant and operationally imminent. This sequential cognitive mechanism provides new evidence of the cognition–action gap in expert cybersecurity decision-making.

LITERATURE REVIEW

To provide a coherent theoretical foundation, this study integrates Technology Threat Avoidance Theory (TTAT) (Liang & Xue, 2009) and the Behavioral Cybersecurity Framework (BCF) (Ait Maalem Lahcen et al., 2020). Together, these frameworks explain how perceptions of cyber risk evolve into protective behavior. Accordingly, this study examines whether Severity Perception influences Cybersecurity Behavior directly or indirectly through Threat Perception. Empirical studies highlight the importance of psychological and organizational factors in promoting secure practices within digital environments (Parsons et al., 2015). The following research question guides the analysis: Which cognitive and perceptual factors influence cybersecurity behavior among digital executives, and how does Threat Perception mediate the relationship between Severity Perception and protective behavior? Figure 1 presents the proposed research model.

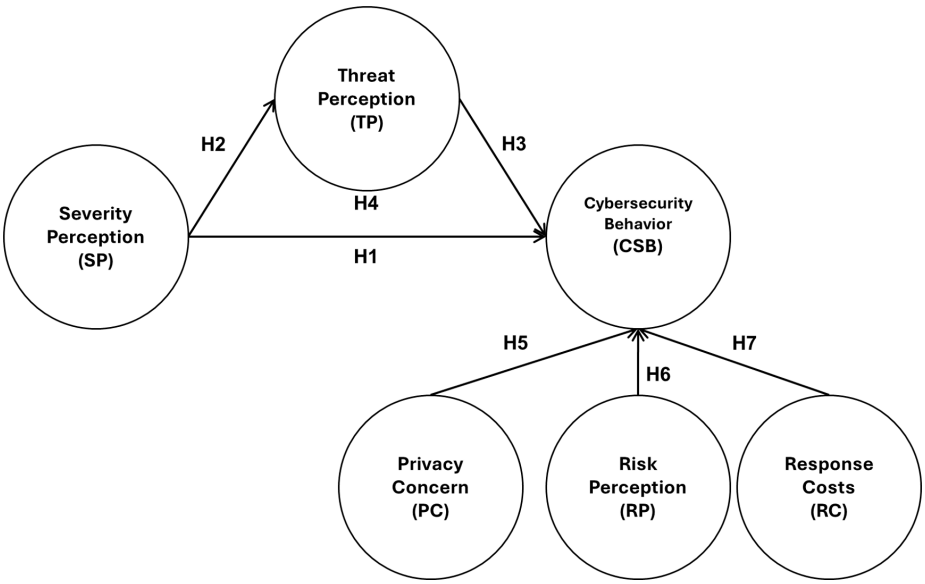

Figure 1. Research Model and Hypothesized Relationships. Source: own elaboration.

Cybersecurity Behavior

Cybersecurity Behavior (CSB) refers to individuals' willingness to adopt practices that protect digital systems and information assets, including compliance with security policies, the use of protective technologies, and proactive risk-mitigation practices (Sutton & Thompson, 2024). Because CSB is shaped by individual perceptions, organizational context, and technological conditions (Kannelønning & Katsikas, 2023), it is conceptualized in this study as the outcome of a cognitive evaluation process in which individuals assess cyber risk severity and interpret their exposure to potential threats.

Based on these arguments, the following hypotheses examine the relationship between severity perception, threat perception, and cybersecurity behavior.

Severity Perception and Cybersecurity Behavior

Severity Perception (SP) refers to an individual's evaluation of the potential that may result from a cyber threat (Latif et al., 2025). Studies indicate that perceived severity can motivate avoidance behavior and protective actions when individuals recognize the consequences of cyber incidents (Alsharida et al., 2025).

However, the literature also indicates that the behavioral effect of severity perception may depend on how individuals interpret the personal relevance of the threat. This phenomenon reflects what recent behavioral cybersecurity research describes as a cognition–action gap, where individuals cognitively recognize cyber risks but do not necessarily translate such awareness into consistent protective behavior. This gap appears particularly relevant among highly specialized users, whose technical expertise may normalize perceptions of cyber risk and reduce the behavioral impact of abstract severity awareness (Greavu-Șerban et al., 2025). In highly specialized professional contexts, recognizing potential damage may not be sufficient to trigger protective action unless the threat is perceived as personally relevant and operationally imminent. Therefore, the following hypothesis is proposed:

H1: *Severity Perception positively influences Cybersecurity Behavior.*

Severity Perception and Threat Perception

Threat Perception (TP) refers to the perceived likelihood and seriousness of experiencing a cyber incident (Wayne & Kostyuk, 2020).

Studies indicate that severity perception contributes to the formation of threat perception by influencing how individuals interpret the potential consequences of cyber risks (Vrhovec & Markelj, 2024).

Empirical evidence shows that when individuals perceive cyber risks as severe, they are more likely to interpret those risks as immediate threats requiring protective responses (Hanifah et al., 2024). Within TTAT models, this cognitive process activates avoidance motivation and encourages protective actions against technological threats. Accordingly, the following hypothesis is proposed:

H2: *Severity Perception positively influences Threat Perception.*

Threat Perception and Cybersecurity Behavior

Threat Perception (TP) is a key predictor of Cybersecurity Behavior (CSB), as it activates psychological mechanisms such as avoidance motivation and personal risk appraisal (Alsharida et al., 2025). In behavioral cybersecurity research, TP is often considered the cognitive trigger that transforms risk awareness into protective action. According to TTAT, TP reflects perceived severity and vulnerability, which motivate individuals to avoid technological risks and adopt protective behaviors such as strong passwords or software updates (Liang & Xue, 2009). Empirical studies in digital environments, including the metaverse and online banking, confirm that TP strongly influences secure behavior and often operates through mechanisms such as self-efficacy, response efficacy, and fear of cyberattacks (Al-Emran et al., 2025). BCF further highlights the role of organizational and social factors, such as internal culture and security policies, in shaping this relationship (Ait Maalem Lahcen, 2020). However, although a higher risk perception may increase the intention to behave securely, its translation into actual behavior depends on perceived personal relevance and response capability (Wayne & Kostyuk, 2020). Recent syntheses confirm the central role of TP in promoting effective cybersecurity behavior (Latif et al., 2025). Therefore, the following hypothesis is proposed:

H3: *Threat perception positively influences Cybersecurity Behavior.*

Mediation of Threat Perception

Severity Perception (SP) positively influences Threat Perception (TP) (Hanifah et al., 2024), which in turn promotes the adoption of secure Cybersecurity Behavior (CSB) (Alsharida et al., 2025; Latif et al., 2025). From a cognitive perspective, the evaluation of potential damage may shape how individuals interpret their exposure to cyber threats, thereby activating protective behavior. Based on this theoretical and empirical evidence, TP is proposed as a mediating mechanism in this relationship. Thus, the following mediation hypothesis is proposed:

H4: *Threat Perception mediates the relationship between Severity Perception and Cybersecurity Behavior.*

Additional Cognitive Drivers of Cybersecurity Behavior

Beyond the central cognitive mechanism analyzed in this study, studies identify complementary factors that may influence cybersecurity behavior.

Privacy Concern and Cybersecurity Behavior

Privacy Concern (PC) refers to individuals' worries about misuse or unauthorized access to personal information in digital environments (Nemec Zlatolas et al., 2024). Higher levels of privacy concern may motivate individuals to adopt stronger protective behaviors, particularly when users perceive potential threats to personal data security (Khan et al., 2021). In organizational contexts, privacy concerns may also influence attitudes toward security technologies and monitoring systems. In this context, the following hypothesis is proposed:

H5: *Privacy Concern positively influences Cybersecurity Behavior.*

Risk Perception and Cybersecurity Behavior

Risk Perception (RP) refers to the subjective evaluation of the likelihood and potential impact of cyber threats, shaped by knowledge, emotions, and prior experiences (Wilson et al., 2020). Higher perceived risk generally encourages more cautious behavior, although

this perception does not always translate directly into protective actions.

The Protection Motivation Theory (PMT) (Rogers, 1975) and TTAT explain that perceived threats and response effectiveness activate the motivation to avoid technological risks. TTAT further emphasizes the role of individual, situational, and organizational risk in this process (Debb & McClellan, 2021). Studies show that higher perceived risk can increase intentions to behave securely, although actual behavioral change depends on facilitators such as awareness and self-efficacy, as well as emotional responses such as fear or anxiety (Goh et al., 2022). Complementarily, TTAT and BCF highlight the psychological and organizational mechanisms underlying the RP→CSB relationship, reinforcing the need for integrated interventions to promote sustainable cybersecurity behaviors. Therefore, the following hypothesis is proposed:

H6: *Risk Perception positively influences Cybersecurity Behavior.*

Response Costs and Cybersecurity Behavior

Response Costs (RC) in cybersecurity refer to the perceived effort, time, resources, or inconvenience associated with adopting protective behaviors against cyber threats (Latif et al., 2025). Studies indicate that RC negatively influences Cybersecurity Behavior (CSB): the higher the perceived cost, the lower the likelihood of adopting secure practices (Al-Emran et al., 2024). According to BCF, RC are considered psychological and organizational barriers, whose effects may be moderated by factors such as self-efficacy and Threat Perception (Dodge et al., 2023). Similarly, the TTAT suggests that individuals evaluate both threats and the costs of protective actions before deciding whether to avoid technological risks, meaning that high RC may inhibit protective behavior even when threats are perceived as serious. However, their impact may be mitigated through self-efficacy, organizational strategies, and targeted behavioral interventions. Within this framework, the following hypothesis is proposed:

H7: *Response Costs negatively influence Cybersecurity Behavior.*

METHODOLOGY

Epistemological Approach and Study Design

This study is grounded in a post-positivist epistemology, which assumes the existence of an objective reality underlying preventive cybersecurity behavior in response to cyber threats while recognizing that this reality cannot be fully known because observations are inevitably influenced by theories, contexts, and measurement instruments (Phillips & Burbules, 2000). Accordingly, a quantitative cross-sectional design was adopted to examine the relationships among the study variables at a single point in time.

Data was analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM), an approach well suited for modeling complex relationships and developing theory under conditions of non-normal data (Hair et al., 2019). To complement the structural model, an Importance–Performance Map Analysis (IPMA) was performed to identify the relative importance and performance of the antecedents of Cybersecurity Behavior and support the prioritization of managerial interventions (Ringle & Sarstedt, 2016).

Data Collection Procedure

The study focused on professionals holding managerial or senior technical positions with direct responsibility for digital decision-making. Digital executives were operationally defined as professionals involved in evaluating technological risks, governing digital infrastructure, approving cybersecurity policies, or allocating resources for digital protection. This definition ensured that the sample consisted of individuals whose cybersecurity behavior could influence organizational resilience. To reduce potential common method bias, participants were assured of anonymity and confidentiality, and the questionnaire explicitly stated that there were no right or wrong answers.

The target population comprised digital professionals working primarily in IT-related functions in Metropolitan Lima, Peru, a group selected because of their high exposure to cyber threats and strategic role in organizational cybersecurity. Most participants reported more

than nine years of professional experience and held technology-related degrees (Table 1). Data was collected through a structured online questionnaire distributed via LinkedIn and professional networks across multiple business sectors. More than 500 professionals involved in digital management, information systems, or cybersecurity-related decision-making were invited to participate. Participation was voluntary and based on informed consent. Eligible respondents held responsibilities related to digital infrastructure, technology management, cybersecurity, or digital decision-making. A total of 311 valid responses were obtained. The non-probabilistic purposive sampling approach may limit generalizability and introduce selection bias; however, it is widely used in studies involving specialized professional populations. The sample size was adequate for PLS-SEM considering the model complexity and number of constructs (Hair et al., 2019). The measurement scales were translated and adapted using a forward–back translation procedure, followed by expert validation and pilot testing to ensure semantic equivalence and cultural suitability for the Peruvian context (Beaton et al., 2000; Brislin, 1970).

Measures and Instruments

The final instrument consisted of 19 items distributed across six theoretical constructs, each measured on a 5-point Likert scale (1 = "strongly disagree" and 5 = "strongly agree"). The scales were adapted from well-established studies in the international literature, thereby ensuring their validity and reliability (Al-Emran et al., 2021; Arachchilage et al., 2016; Li et al., 2020).

Ethical Considerations

The study adhered to the scientific research ethical principles established by the University of Lima's Graduate School. All participants signed an informed consent form prior to their participation, ensuring their understanding of the study's purpose, the voluntary nature of their involvement, and the confidentiality of their responses.

Furthermore, the research was reviewed and approved by the Integrity and Ethics Committee under registration number EPG-DA1-008-2024, ensuring compliance with institutional ethical standards and the protection of participants' rights.

RESULTS

Evaluation of the Measurement Model

The measurement model was evaluated by examining indicator reliability, internal consistency, and convergent validity. Although some factor loadings were slightly below the recommended threshold of 0.70, they were retained because composite reliability and convergent validity remained satisfactory, consistent with established PLS-SEM guidelines (Hair et al., 2019). As shown in Table 2, all constructs achieved acceptable levels of reliability and convergent validity.

High outer loadings generally reflect strong conceptual homogeneity among indicators, although they may also indicate limited variability. A particular consideration concerns the Risk Perception (RP) construct, measured with two indicators showing markedly asymmetric loadings (0.588 and 0.995). Although composite reliability and convergent validity met the recommended thresholds, this pattern suggests limited conceptual variability and possible redundancy. In highly specialized executive populations, cyber risk perceptions may become normalized through extensive technical experience, partially explaining this asymmetry. Accordingly, the RP construct should be interpreted with caution, and future studies are encouraged to incorporate additional indicators capturing broader dimensions of cyber risk appraisal.

All AVE values exceeded the recommended threshold of 0.50, confirming convergent validity.

Discriminant validity was confirmed using both the Fornell–Larcker criterion (Table 3) and the HTMT ratio (Table 4). In all cases, the square root of the AVE exceeded the inter-construct correlations and HTMT values remained below the conservative threshold of 0.85, confirming that the constructs are empirically distinct.

Table 1. Descriptive characteristics of the sample.

Sex	Male	72.6%
	Female	27.4%
Age	20-29 years old	11.9%
	30-39 years old	33.8%
	40-49 years old	29.3%
	50-59 years old	19.9%
	+ 60 years old	5.1%
Profession	Systems or IT engineer	53.7%
	Administrator	12.2%
	Lawyer	9.0%
	Industrial engineer	7.1%
	Electronic engineer	4.5%
	Others	13.5%
Level of education	Master's degree	58.8%
	Professional degree	36.3%
	Doctorate	3.2%
	Technical degree	1.6%
Work experience	0-3 years	5.10%
	3-6 years	11.3%
	6-9 years	10.6%
	+ 9 years	73.0%
Sector	Services	30.2%
	Financial	24.1%
	Public	10.6%
	Industry	9.3%
	Retail	4.5%
	Education	4.2%
	Telecommunications	3.2%
	Health	2.3%
	Others	11.6%

Source: own elaboration.

Although some constructs were measured with two indicators, this specification is acceptable in PLS-SEM when reliability and convergent validity satisfy recommended thresholds. Two-item constructs have been shown to provide stable measurement for theoretically well-defined constructs and parsimonious models (Hair et al., 2021; Sarstedt et al., 2021).

Common method bias and potential inflation associated with socially desirable responding were assessed using the full collinearity test. Following Kock (2015), all VIF values ranged from 1.000 to 1.858, remaining well below the threshold of 3.3 and indicating that common method bias was unlikely to substantially affect the model estimates (Table 5).

Overall, the measurement model demonstrated adequate reliability and validity, supporting the subsequent evaluation of the structural model.

Table 2. Factor loadings, reliability and convergent validity.

Construct	Item	Loads	Alpha	CR	AVE
Cybersecurity Behavior	CSB1	0.672	0.703	0.81	0.517
	CSB2	0.668			
	CSB3	0.806			
	CSB4	0.720			
Privacy Concern	PC1	0.806	0.757	0.86	0.673
	PC2	0.870			
	PC3	0.782			
Risk Perception	RP1	0.588	0.752	0.753	0.528
	RP3	0.995			
Severity Perception	SP1	0.800	0.615	0.788	0.557
	SP2	0.606			
	SP 3	0.814			
Threat Perception	TP1	0.895	0.877	0.924	0.803
	TP2	0.902			
	TP3	0.891			
Response Cost	RC1	0.842	0.756	0.857	0.666
	RC2	0.801			
	RC3	0.805			

Source: own elaboration.

Table 3. Fornell and Larcker Criteria.

	CSB	PC	RP	SP	TP	RC
CSB	0.719					
PC	0.213	0.820				
RP	0.120	0.561	0.817			
SP	0.251	0.499	0.329	0.746		
TP	0.357	0.521	0.406	0.541	0.896	
RC	-0.128	0.063	0.245	0.017	0.005	0.816

Notes: CSB = Cybersecurity Behavior; PC = Privacy Concern; RP = Risk Perception; SP = Severity Perception; TP = Threat Perception; RC = Response Costs.
Source: own elaboration.

Table 4. Heterotrait-Monotrait ratio of correlations.

	CSB	PC	RP	SP	TP	RC
CSB						
PC	0.281					
RP	0.130	0.787				
SP	0.334	0.725	0.538			
TP	0.412	0.636	0.449	0.696		
RC	0.158	0.117	0.444	0.132	0.090	

Notes: CSB = Cybersecurity Behavior; PC = Privacy Concern; RP = Risk Perception; SP = Severity Perception; TP = Threat Perception; RC = Response Costs. All HTMT values are below the conservative threshold of 0.85, supporting discriminant validity.
Source: own elaboration.

Structural Model

After confirming the adequacy of the measurement model, the structural model was evaluated. Collinearity diagnostics showed no multicollinearity concerns, with VIF values ranging from 1.000 to 1.858, well below the conservative threshold of 3.3 (Hair et al., 2019) (Table 5).

The model explained 15.0% of the variance in Cybersecurity Behavior (CSB) and 29.3% of the variance in Threat Perception (TP). Positive Q^2 values (CSB = 0.044; TP = 0.272) supported the model's predictive relevance (Table 6). Although the explained variance is modest, it is consistent with behavioral research involving executive decision-making, where behavior is simultaneously influenced by cognitive, organizational, and contextual factors.

The analysis of path coefficients revealed an important pattern. Severity Perception (SP) did not have a significant direct effect on Cybersecurity Behavior (SP → CSB; $\beta = 0.078$; $p = 0.342$), representing a central empirical finding of the study.

In contrast, Severity Perception strongly influenced Threat Perception (SP → TP; $\beta = 0.541$; $p < 0.001$), while Threat Perception significantly predicted Cybersecurity Behavior (TP → CSB; $\beta = 0.305$; $p = 0.002$).

Privacy Concern (PC), Risk Perception (RP), and Response Costs (RC) did not show significant direct effects on CSB. Specifically, PC ($\beta = 0.032$; $p = 0.674$) and RP ($\beta = -0.016$; $p = 0.830$) were non-significant, whereas RC showed a negative but marginal effect ($\beta = -0.129$; $p = 0.067$). Consequently, H5, H6, and H7 were not supported.

Given the non-significant direct relationship between Severity Perception and Cybersecurity Behavior, a mediation analysis was conducted to examine the indirect role of Threat Perception.

Table 5. Collinearity

Variable	VIF
PC -> CSB	1.858
RP -> CSB	1.61
SP -> CSB	1.557
SP -> TP	1
TP -> CSB	1.647
RC -> CSB	1.079

Notes: CSB = Cybersecurity Behavior; PC = Privacy Concern; RP = Risk Perception; SP = Severity Perception; TP = Threat Perception; RC = Response Costs.
Source: own elaboration.

Table 6. Results of the structural model: path coefficients, significance, and R^2 and Q^2 values.

Hypothesis	β	SD	t-Statistic	p-Value	Decision	R^2	Q^2
H1: SP -> CSB	0.078	0.082	0.951	0.342	Not Supported		
H2: SP -> TP	0.541	0.077	7.060	0	Supported		
H3: TP -> CSB	0.305	0.099	3.092	0.002	Supported		
H5: PC -> CSB	0.032	0.077	0.421	0.674	Not Supported		
H6: RP -> CSB	-0.016	0.075	0.215	0.830	Not Supported		
H7: RC -> CSB	-0.129	0.070	1.834	0.067	Not Supported		
CSB						0.150	0.044
TP						0.293	0.272

Notes: CSB = Cybersecurity Behavior; PC = Privacy Concern; RP = Risk Perception; SP = Severity Perception; TP = Threat Perception; RC = Response Costs.
Source: own elaboration.

Mediation Analysis

To examine the cognitive mechanism linking Severity Perception and Cybersecurity Behavior, a mediation analysis was conducted.

Threat Perception significantly mediated the relationship between Severity Perception and Cybersecurity Behavior ($\beta = 0.165$; $t = 2.775$; $p = 0.006$), supporting Hypothesis 4 (Table 7). Given the non-significant direct effect (SP → CSB) and the significant indirect effect through TP, the results indicate that Severity Perception influences cybersecurity behavior only indirectly through Threat Perception.

This finding identifies a sequential cognitive mechanism in which awareness of cyber risk contributes to protective behavior only when translated into a personally relevant perception of threat. The theoretical implications of this mechanism are discussed in the following section.

Table 7. Mediation analysis.

Mediation route	β	SD	t-Statistic	p-Value	Decision
H4: SP -> TP -> CSB	0.165	0.060	2.775	0.006	Supported

Notes: CSB = Cybersecurity Behavior; SP = Severity Perception; TP = Threat Perception.
Source: own elaboration

Importance-Performance Map Analysis (IPMA)

To complement the structural model, an Importance–Performance Map Analysis (IPMA) was conducted to identify managerial priorities by jointly assessing the relative importance and performance of each construct.

As shown in Table 8 and Figure 2, Threat Perception exhibited the highest importance (0.279) and one of the highest performance levels (90.000), whereas Severity Perception showed moderate importance (0.114) with relatively high performance (83.211). Privacy Concern demonstrated high performance but low importance.

Response Costs represented the main managerial improvement opportunity. Although its direct effect on Cybersecurity Behavior was not statistically significant, it exhibited the lowest performance level (42.142), suggesting the presence of operational barriers that may hinder the adoption of secure practices.

Overall, the IPMA complements the structural model by identifying organizational priorities for cybersecurity interventions, thereby

facilitating the translation of structural model findings into actionable managerial priorities.

Table 8. Importance-Performance Map Analysis (IPMA).

Variable	Importance of CSB	LV Performance
PC	0.028	86.811
RP	-0.017	78.446
SP	0.114	83.211
TP	0.279	90.000
RC	-0.129	42.142

Notes: PC = Privacy Concern; RP = Risk Perception; SP = Severity Perception; TP = Threat Perception; RC = Response Costs.
Source: own elaboration.

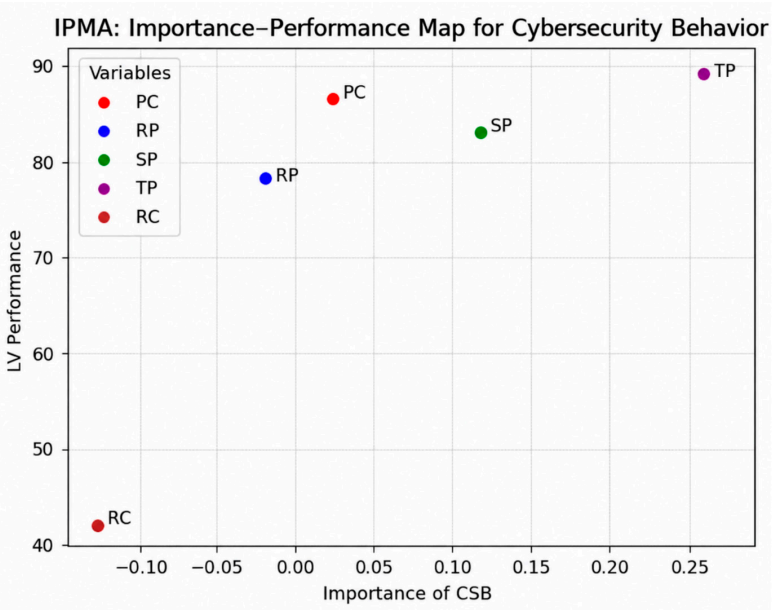

Figure 2. Importance–Performance Map of the Determinants of Cybersecurity Behavior
Note. PC = Privacy Concern; RP = Risk Perception; SP = Severity Perception; TP = Threat Perception; RC = Response Costs. Source: own elaboration.

DISCUSSION

This study examined the cognitive mechanisms underlying Cybersecurity Behavior among digital executives, focusing on whether Threat Perception mediates the relationship between Severity Perception and Cybersecurity Behavior. The findings identify Threat Perception as the key mechanism translating cyber risk awareness into protective behavior. Although the model explains a modest proportion of variance (R^2 = 0.15), this level is consistent with behavioral research, where decision-making is shaped by multiple contextual and psychological factors.

For H1 (SP→CSB), no significant relationship was found. This result differs from studies suggesting that severity directly motivates protective action (Alsharida et al., 2025). A plausible explanation lies in the expert profile of participants, who were predominantly IT specialists with high digital exposure and extensive professional experience. As shown in Table 1, 73% reported more than nine years

of experience and 53.7% were systems or technology engineers, indicating a population with substantial technical expertise and professional familiarity with cybersecurity issues.

This discrepancy may reflect differences in the populations examined across prior studies, which have primarily focused on general users such as online banking customers, employees, or students (Alrawhani et al., 2025; Arachchilage et al., 2016). In contrast, digital executives combine extensive technical expertise with strategic decision-making responsibilities, suggesting that established behavioral relationships may operate differently in expert populations. Rather than responding to general warnings, experts tend to evaluate cyber risks through analytical reasoning and situational cues derived from experience, an effect consistent with the expertise bias described by Greavu-Șerban et al. (2025).

Accordingly, Severity Perception among expert users appears to function primarily as contextual information rather than a direct behavioral trigger. Protective behavior is activated when threats are perceived as imminent, personally relevant, and directly connected to organizational responsibilities, helping explain the non-significant SP→CSB relationship.

Consistent with TTAT and PMT, Severity Perception strongly influenced Threat Perception (H2), while Threat Perception significantly predicted Cybersecurity Behavior (H3), supporting prior behavioral cybersecurity research (Alsharida et al., 2025; Boss et al., 2015; Latif et al., 2025). Together, these findings indicate that severity contributes to threat appraisal, whereas Threat Perception activates protective behavior when cyber risks are interpreted as operationally relevant within the executive decision-making context.

The principal theoretical contribution emerged in H4, where Threat Perception significantly mediated the relationship between Severity Perception and Cybersecurity Behavior. Consistent with TTAT, PMT, and the Behavioral Cybersecurity Framework, the findings indicate that Severity Perception initiates threat appraisal, whereas Threat Perception transforms this evaluation into protective behavior (Hanifah et al., 2024). Among technically experienced executives, cyber risk awareness alone is insufficient unless threats are perceived as personally relevant and operationally imminent.

This mediation can be interpreted through the sequential cognitive logic underlying the Technology Threat Avoidance Theory (TTAT) and the Behavioral Cybersecurity Framework. Freom this perspective, Severity Perception represents an initial evaluation of potential damage, while Threat Perception transforms this evaluation into a personal assessment of vulnerability that activates protective behavior. In practical terms, the results suggest a cognitive sequence in which recognition of severity leads to threat interpretation and subsequently to behavioral activation. Threat Perception therefore operates as the psychological mechanism that translates technical knowledge about cyber risks into preventive action.

Technically experienced professionals may recognize severe cyber risks, yet protective behavior is more likely to occur when those risks are interpreted as concrete and situational threats within their organizational environment. This dynamic helps explain the expertise bias observed in the sample: technical knowledge may normalize perceptions of severity, whereas behavioral activation depends on situational threat interpretation.

The Importance–Performance Map Analysis (IPMA) complemented the structural model by identifying managerial priorities for cybersecurity interventions. Rather than providing additional theoretical evidence, the IPMA served as a decision-support tool for identifying constructs requiring greater organizational attention based on their relative importance and performance. Threat Perception exhibited the highest importance ($\beta = 0.279$) together with high performance (~90.0), reinforcing its central role in cybersecurity behavior. In contrast, Response Costs showed the lowest performance (42.14) and a negative path coefficient ($\beta = -0.129$). Although its relationship with Cybersecurity Behavior did not reach conventional statistical significance ($p = 0.067$), the result suggests a marginal structural trend indicating that perceived operational effort may still discourage protective behavior among digital executives. This interpretation is consistent with the IPMA results and with prior

research within the Behavioral Cybersecurity Framework, which identifies Response Costs as psychological and organizational barriers that may inhibit secure behavior even when their direct effects are relatively weak (Dodge et al., 2023).

Finally, H5, H6, and H7 (PC→CSB, RP→CSB, and RC→CSB) did not show significant direct effects. These findings are consistent with similar previous research where general cognitive evaluations do not necessarily translate into protective behavior (Dodge et al., 2023; Greavu-Şerban et al., 2025). Together, these results suggest that, among digital executives, Threat Perception exerts greater behavioral influence than broader cognitive evaluations such as Privacy Concern or Risk Perception.

Overall, the findings contribute at three complementary levels. Theoretically, they extend the Technology Threat Avoidance Theory (TTAT) and the Behavioral Cybersecurity Framework (Ait Maalem Lahcen et al., 2020; Liang & Xue, 2009) by demonstrating that, among technically experienced digital executives, Threat Perception—rather than Severity Perception alone—serves as the cognitive mechanism translating cyber risk awareness into protective behavior. Empirically, the study provides evidence from an underexplored population of digital executives in Peru, showing how technical expertise may reshape established behavioral relationships. From a managerial perspective, the findings suggest that organizations should strengthen the perceived immediacy and personal relevance of cyber threats while reducing operational barriers that hinder the adoption of secure practices.

Management Implications

The findings provide practical guidance for organizational leaders seeking to strengthen cybersecurity culture from a behavioral perspective. Among experienced digital executives, Threat Perception emerged as the primary driver of Cybersecurity Behavior, suggesting that organizations should move beyond technical training and strengthen the perceived immediacy and personal relevance of cyber threats. For highly specialized professionals, risk communication is most effective when linked to business processes, operational impacts, and managerial responsibilities.

The structural model and the IPMA provide complementary managerial insights. Whereas the structural model identifies the strongest behavioral drivers, the IPMA highlights areas with the greatest improvement potential. Accordingly, although Response Costs did not show a statistically significant direct effect, their low performance suggests operational barriers that deserve managerial attention.

In digitally intensive environments, secure practices often compete with operational efficiency. Organizations should therefore reduce operational friction by simplifying authentication procedures, increasing automation, integrating security mechanisms into daily workflows, and complementing awareness initiatives with contextualized threat communication and executive-oriented cyber simulations. Together, these actions strengthen the translation of cybersecurity awareness into consistent protective behavior.

For CISOs and organizational leaders, three priorities emerge: (1) emphasize the personal relevance and operational immediacy of cyber threats; (2) reduce operational friction by simplifying and integrating security controls into executive workflows; and (3) reinforce secure decision-making through realistic executive cyber simulations.

Beyond organizational practice, these findings also have implications for cybersecurity governance and public policy. National cybersecurity agencies, sector regulators, and corporate governance bodies could complement compliance-oriented cybersecurity requirements with behavioral approaches that strengthen executive decision-making. In emerging digital economies such as Peru, executive awareness programs should emphasize the immediacy and personal relevance of cyber threats while incorporating behavioral design principles into cybersecurity governance frameworks to strengthen organizational resilience.

Theoretical Implications

This study extends the Technology Threat Avoidance Theory (TTAT) (Liang & Xue, 2009) and the Behavioral Cybersecurity

Framework (BCF) (Ait Maalem Lahcen et al., 2020) by explaining the cognitive mechanisms underlying Cybersecurity Behavior (CSB) among digital executives.

First, consistent with TTAT, the findings confirm that Threat Perception (TP) functions as the key cognitive mediator between Severity Perception (SP) and cybersecurity behavior, indicating that recognizing potential damage alone does not necessarily trigger protective action. This finding extends TTAT by empirically supporting the sequential cognitive process underlying technology avoidance.

Second, in line with the BCF, the results suggest that cybersecurity decisions are shaped by the interaction between perceived threats and Response Costs (RC). The finding that perceived operational effort may hinder secure practices reinforces the theoretical relevance of operational barriers within behavioral models of cybersecurity.

In addition, the Importance–Performance Map Analysis (IPMA) complements these theoretical perspectives by identifying the relative importance and performance of the determinants of cybersecurity behavior, providing an additional empirical perspective on the practical application of these theories in digital executive environments.

Overall, the findings extend the applicability of TTAT and the BCF by demonstrating that Threat Perception mediates the relationship between Severity Perception and protective behavior, while Response Costs may constrain the consistent adoption of secure practices.

Limitations and Future Research

Although this study provides relevant insights into the cognitive drivers of Cybersecurity Behavior (CSB) among digital executives, several limitations should be acknowledged.

First, the non-probabilistic purposive sample, composed primarily of highly experienced IT professionals with postgraduate education and more than nine years of professional experience, may limit the generalizability of the findings. Although this profile is appropriate for examining individuals with high digital exposure and cybersecurity decision-making responsibilities, caution is warranted when extending the results to less technically specialized populations. Future research should employ probabilistic sampling and comparative designs across occupational groups to assess the robustness of the observed behavioral patterns. In addition, the use of self-reported data may still be affected by social desirability bias despite the procedural and statistical controls implemented. Although the full collinearity assessment indicated that systematic response inflation was unlikely to substantially affect the model estimates, no dedicated psychometric instrument was included to directly measure socially desirable responding. Future studies could therefore strengthen methodological rigor by incorporating validated social desirability scales.

Second, the cross-sectional design does not permit causal inference or the examination of temporal relationships among the constructs. Although the structural model identifies statistically significant associations consistent with the proposed theoretical framework, dynamic and reciprocal relationships cannot be fully captured. For example, repeated engagement in protective behaviors may reduce perceived Response Costs over time, whereas persistent operational friction may discourage those behaviors. Longitudinal studies are therefore needed to examine how Threat Perception, Severity Perception, and Cybersecurity Behavior evolve following cyber incidents or organizational changes. Furthermore, the structural relationships identified may also be influenced by organizational or contextual variables not included in the present model, such as security culture, leadership support, prior cyber incident exposure, or the institutional cybersecurity climate. Consequently, although the proposed relationships are theoretically grounded, the findings should be interpreted as theoretically consistent associations rather than definitive causal effects.

Third, although the proposed model provides meaningful insights into the cognitive mechanisms underlying Cybersecurity Behavior, its explanatory power was modest ($R^2 = 0.150$), indicating that a substantial proportion of executive cybersecurity behavior remains influenced by factors beyond the cognitive constructs examined in this study. This finding reflects the complexity of cybersecurity decision-

making, where individual, organizational, and contextual factors jointly shape protective behavior. Future research should extend the model by incorporating additional variables such as digital self-efficacy, social norms, security climate, technology fatigue, trust in management, and prior cyber incident experience. Measurement robustness could also be enhanced by expanding the number of indicators for selected constructs, particularly Risk Perception, which was measured with only two indicators displaying asymmetric loadings. Although acceptable reliability and convergent validity were achieved, additional indicators would provide a more comprehensive assessment of this construct.

Fourth, future research should complement these findings through longitudinal, experimental, and cross-contextual designs. Longitudinal studies would clarify how cybersecurity perceptions and behaviors evolve over time, whereas experimental designs could isolate the causal effects of operational conditions by exposing participants to simulated phishing or social engineering scenarios combined with real-time workflow interruptions or varying levels of security procedure complexity. Such approaches would provide stronger evidence regarding the influence of Response Costs on executive cybersecurity behavior. Cross-national and cross-sector comparisons would further clarify how cultural, regulatory, and organizational contexts shape cybersecurity behavior, contributing to the development of more generalizable behavioral models.

Overall, these directions reinforce the need to approach cybersecurity not only as a technical challenge but also as a behavioral, managerial, and organizational capability in which individual perceptions, organizational processes, and system design jointly shape secure behavior.

CONCLUSIONS

The study demonstrates that, even among digital executives with strong technical expertise, protective cybersecurity behavior is not triggered by the abstract severity of cyber risks but by their personal interpretation as immediate and relevant threats. Based on a sample composed primarily of highly experienced IT professionals, the findings confirm that Threat Perception (TP) is the strongest predictor of Cybersecurity Behavior (CSB) and the cognitive mechanism through which Severity Perception (SP) is translated into preventive action. In other words, executives do not act simply because they recognize that cyber risks are severe, but because they perceive those risks as imminent, plausible, and directly relevant to their organizational responsibilities.

The study makes three complementary contributions. The findings demonstrate that, among technically experienced digital executives, awareness of potential damage alone is insufficient to activate protective behavior. Instead, action emerges when cyber risks are cognitively reframed as personally relevant threats. This evidence extends the explanatory scope of the Technology Threat Avoidance Theory (TTAT) by showing that Threat Perception functions as the cognitive bridge between cyber risk awareness and behavioral activation in expert populations. The study also contributes to the Behavioral Cybersecurity Framework (BCF) by reinforcing the importance of cognitive mechanisms in explaining secure behavior among highly specialized professionals.

The findings also provide new empirical evidence from an underexplored population of digital executives in Peru, illustrating how technical expertise may reshape behavioral relationships traditionally observed in general user populations. The Importance–Performance Map Analysis (IPMA) complements these findings by identifying Threat Perception as the highest managerial priority while highlighting Response Costs as a potential source of operational friction. Although Response Costs did not show a statistically significant direct effect, its low score suggests opportunities to simplify security procedures and facilitate the consistent adoption of secure practices.

From a managerial perspective, the findings suggest that effective cybersecurity strategies should extend beyond technical controls and compliance requirements. Organizations should strengthen the perceived immediacy and personal relevance of cyber threats while simultaneously reducing operational barriers that discourage secure behavior. This behavioral perspective positions cybersecurity not merely as a technical function, but as a

strategic managerial capability that strengthens organizational resilience by improving executive decision-making in increasingly complex digital environments.

Conflict of interest declaration:

The authors declare that they have no conflicts of interest.

Funding:

The authors did not receive funding to conduct this research.

Use of Artificial Intelligence (AI):

The authors acknowledge receiving assistance from AI to improve the English writing of this document.

Authors' contributions:

Conceptualization and Data Curation: FAV; Formal Analysis: FAV and DNC; Research: FAV; Methodology, Software, Supervision, Validation: FAV and DNC; Visualization, Writing - Original Draft, and Writing - Review and Editing: FAV.

All authors have read and accepted the published version of the manuscript.

REFERENCES

Ait Maalem Lahcen, R., Caulkins, B. D., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity, 3*(1), 1-16. https://doi.org/10.1186/s42400-020-00052-2

Al-Emran, M., Al-Sharafi, M. A., Foroughi, B., Iranmanesh, M., Alsharida, R. A., Al-Qaysi, N., & Ali, N. A. (2024). Evaluating the barriers affecting cybersecurity behavior in the metaverse using PLS-SEM and fuzzy sets (fsQCA). *Computers in Human Behavior, 159*, 108315. https://doi.org/10.1016/j.chb.2024.108315

Al-Emran, M., Granic, A., Al-Sharafi, M. A., Ameen, N., & Sarrab, M. (2021). Examining the roles of students' beliefs and security concerns for using smartwatches in higher education. *Journal of Enterprise Information Management, 34*(4), 1229–1251. https://doi.org/10.1108/JEIM-02-2020-0052

Alsharida, R., Al-Rimy, B., Al-Emran, M., Al-Sharafi, M., & Zainal, A. (2025). Predicting cybersecurity behaviors in the metaverse through the lenses of TTAT and TPB: a hybrid SEM-ANN approach. *Online Information Review*. https://doi.org/10.1108/oir-08-2023-0425

Alrawhani, E. M., Romli, A., & Al-Sharafi, M. A. (2025). Evaluating the role of protection motivation theory in information security policy compliance: Insights from the banking sector using PLS-SEM approach. *Journal of Open Innovation: Technology, Market, and Complexity*, *11*(1), 100463. https://doi.org/10.1016/j.joitmc.2024.100463

Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior, 60*, 185–197. https://doi.org/10.1016/j.chb.2016.02.065

Beaton, D. E., Bombardier, C., Guillemin, F., & Ferraz, M. B. (2000). Guidelines for the process of cross-cultural adaptation of self-report measures. *Spine, 25*(24), 3186–3191. https://doi.org/10.1097/00007632-200012150-00014

Bishop, L. M., Asquith, P. M., & Morgan, P. L. (2025). The employee cybersecurity awareness framework. *Human Behavior and Emerging Technologies, 2025*, 1025045. https://doi.org/10.1155/hbe2/1025045

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors1. *MIS Quarterly*, *39*(4), 837-864. https://doi.org/10.25300/MISQ/2015/39.4.5

Brislin, R. W. (1970). Back-translation for cross-cultural research. *Journal of Cross-Cultural Psychology, 1*(3), 185–216. https://doi.org/10.1177/135910457000100301

Debb, S. M., & McClellan, M. K. (2021). Perceived vulnerability as a determinant of increased risk for cybersecurity risk behavior. *Cyberpsychology, Behavior, and Social Networking*, *24*(9), 605-611. https://doi.org/10.1089/cyber.2021.0043

Dodge, C., Fisk, N., Burruss, G., Moule, R., & Jaynes, C. (2023). What motivates users to adopt cybersecurity practices? A survey experiment assessing protection motivation theory. *Criminology & Public Policy, 22*, 849-868. https://doi.org/10.1111/1745-9133.12641

Goh, Z. H., Hou, M., & Cho, H. (2022). The impact of a cause–effect elaboration procedure on information security risk perceptions: a construal fit perspective. *Journal of Cybersecurity*, *8*(1), tyab026. https://doi.org/10.1093/cybsec/tyab026

Greavu-Șerban, V., Constantin, F., & Necula, S.-C. (2025). Exploring heuristics and biases in cybersecurity: A factor analysis of social engineering vulnerabilities. *Systems, 13*(4), 280. https://doi.org/10.3390/systems13040280

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2-24. https://doi.org/10.1108/EBR-11-2018-0203

Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Danks, N., & Ray, S. (2021). *Partial least squares structural equation modeling (PLS-SEM) using R: A workbook*. Springer. https://doi.org/10.1007/978-3-030-80519-7

Hanifah, H., Vafaei-Zadeh, A., Teoh, K., & Nikbin, D. (2024). Cybersecurity awareness and fear of cyberattacks among online banking users in Malaysia. *International Journal of Bank Marketing, 43*(3), 476-505. https://doi.org/10.1108/ijbm-03-2024-0138

Kannelønning, K., & Katsikas, S. (2023). A systematic literature review of how cybersecurity-related behavior has been assessed. *Information & Computer Security, 31*(4), 463-477. https://doi.org/10.1108/ics-08-2022-0139

Khan, N., Ikram, N., Murtaza, H., & Asadi, M. (2021). Social media users and cybersecurity awareness: predicting self-disclosure using a hybrid artificial intelligence approach. *Kybernetes, 52*(1), 401-421. https://doi.org/10.1108/k-05-2021-0377

Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of e-Collaboration*, 11(4), 1–10. https://doi.org/10.4018/ijec.2015100101

Latif, S., Sulaiman, N., Aziz, N., Yacob, A., & Nasir, A. (2025). Development of cybersecurity awareness model based on protection motivation theory (PMT) for digital IR 4.0 in Malaysia. *International Journal of Advanced Computer Science and Applications, 16*(3). https://doi.org/10.14569/ijacsa.2025.01603117

Li, K., Cheng, L., & Teng, C. I. (2020). Voluntary sharing and mandatory provision: Private information disclosure on social networking sites. *Information Processing & Management, 57*(1), Article 102128. https://doi.org/10.1016/J.IPM.2019.102128

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, 33, 71-90. https://doi.org/10.2307/20650279

Nemec Zlatolas, L., Welzer, T., & Lhotska, L. (2024). Data breaches in healthcare: security mechanisms for attack mitigation. *Cluster Computing, 27*(2), 123-145. https://doi.org/10.1007/s10586-024-04012-2

Parsons, K., Young, E., Butavicius, M., McCormac, A., Pattinson, M., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making*, 9, 117 - 129. https://doi.org/10.1177/1555343415575152

Phillips, D. C., & Burbules, N. C. (2000). *Postpositivism and educational research*. Rowman & Littlefield Publishers.

Ringle, C. M., & Sarstedt, M. (2016). Gain more insight from your PLS-SEM results: The importance-performance map analysis. *Industrial management & data systems*, *116*(9), 1865-1886. https://doi.org/10.1108/IMDS-10-2015-0449

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Sarstedt, M., Ringle, C. M., & Hair, J. F. (2021). Partial least squares structural equation modeling. In C. Homburg, M. Klarmann, A. Vomberg, & A. Kannan (Eds.), *Handbook of market research (pp. 587-632)*. Springer. https://doi.org/10.1007/978-3-319-57413-4_15

Sutton, A., & Thompson, L. (2024). Towards a cybersecurity culture-behaviour framework: A rapid evidence review. *Computers & Security, 148*, 104110. https://doi.org/10.1016/j.cose.2024.104110

Vrhovec, S., & Markelj, B. (2024). We need to aim at the top: Factors associated with cybersecurity awareness of cyber and information security decision-makers. *Plos one*, *19*(10), e0312266. https://doi.org/10.1371/journal.pone.0312266

Wayne, C., & Kostyuk, N. (2020). The micro foundations of state cybersecurity: Cyber risk perceptions and the mass public. *Journal of Global Security Studies, 5*(1), 1-19. https://doi.org/10.1093/jogss/ogz077

Wilson, C., Onibokun, J., Schaik, P., Jansen, J., & Renaud, K. (2020). Risk as affect: The affect heuristic in cybersecurity. *Computers & Security, 90*, 101651. https://doi.org/10.1016/j.cose.2019.101651