OPEN ACCESS
Jurnal Ilmiah Ilmu Terapan Universitas Jambi
Vol. 10 No. 2. April 2026, pp. 1114-1131 DOI. 10.22437/jiituj.v10i2.54776

Review Article

EXTENDING PROTECTION MOTIVATION THEORY TO EXPLAIN ORGANIZATIONAL CYBERSECURITY BEHAVIOR: A SYSTEMATIC LITERATURE REVIEW

Susyanto[1,*], Rita Yuni Mulyanti[2], Nova Rini[3]

[1] Muhammadiyah University of Technology Jakarta, Jakarta, Indonesia
Corresponding author email: susyanto0o@gmail.com

Article Info
Received: Feb 11, 2026
Revised: Mar 08, 2026
Accepted: Apr 25, 2026
OnlineVersion: Apr 30, 2026

Abstract
The increasing complexity of cyber threats highlights the critical role of human behavior in ensuring organizational cybersecurity, yet existing research remains conceptually fragmented. This study aims to systematically synthesize and extend the application of Protection Motivation Theory (PMT) in explaining organizational cybersecurity behavior by integrating protection habit and cybersecurity awareness into a unified framework. A Systematic Literature Review (SLR) was conducted following PRISMA 2020 guidelines. Peer-reviewed studies published between 2015 and 2025 were retrieved from Scopus-indexed and major academic databases using structured Boolean search strategies. After screening and eligibility assessment, 35 studies were selected and analyzed using thematic and narrative interpretative synthesis. The results indicate that coping appraisal, particularly self-efficacy, consistently exerts a stronger influence on cybersecurity behavior than threat appraisal. In addition, cybersecurity awareness enhances cognitive interpretation of threats and coping mechanisms, while protection habit reinforces sustained behavioral compliance over time. These findings suggest that PMT operates as a dynamic and iterative motivational system rather than a static cognitive framework. This study contributes theoretically by extending PMT through the integration of behavioral reinforcement and cognitive translation mechanisms, resulting in a more comprehensive behavioral-system model. Practically, the findings highlight the importance of designing cybersecurity strategies that prioritize employee capability development, awareness enhancement, and habit formation to achieve long-term organizational resilience.

Keywords: Cybersecurity Awareness, Cybersecurity Behavior, Protection Motivation Theory, Self-Efficacy, Systematic Literature Review.

© 2026 by the author(s)
This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

INTRODUCTION

Despite the rapid growth of cybersecurity behavior research, the existing literature remains conceptually fragmented. While Protection Motivation Theory (PMT) has been widely used to explain individual security behavior, prior studies tend to focus on isolated psychological determinants such as

threat perception, self-efficacy, and awareness, without providing a comprehensive integration of these constructs (Sommestad & Hallberg, 2015; Kiran et al., 2025a).

Furthermore, existing studies often examine cybersecurity behavior in specific contexts or industries, limiting generalizability and theoretical consolidation. For instance, several studies emphasize the role of self-efficacy and response efficacy in shaping protective behavior, yet these findings are frequently presented in isolation without integrating broader behavioral and contextual mechanisms (Li et al., 2022; Alrawhani et al., 2025). In addition, emerging constructs such as cybersecurity awareness and protection habit have been identified as important factors influencing security behavior, but their interaction with core PMT components has not been systematically synthesized (Zwilling et al., 2022; Lee & Lee, 2023).This lack of integrative synthesis highlights a critical gap in the literature.

Addressing this gap is increasingly important as organizations face complex and evolving cyber threats that cannot be effectively mitigated through technological solutions alone (Khoza et al., 2024a). Prior research consistently demonstrates that human behavior remains a key vulnerability in cybersecurity systems, particularly in the context of social engineering attacks and policy non-compliance (Kuraku et al., 2023; Baltuttis et al., 2024). Therefore, understanding how cognitive processes, behavioral reinforcement, and contextual factors interact is essential for developing more effective cybersecurity strategies. Without a systematic synthesis of these elements, existing knowledge remains fragmented and difficult to translate into practice.

To address these limitations, this study employs a Systematic Literature Review (SLR) based on PRISMA 2020 guidelines to systematically identify, evaluate, and synthesize prior research on cybersecurity behavior within the framework of Protection Motivation Theory. This study further extends PMT by integrating cybersecurity awareness and protection habit as key constructs that enhance its explanatory power in organizational contexts.

Therefore, this study aims to: 1) systematically review and synthesize existing literature on cybersecurity behavior within the Protection Motivation Theory framework; 2) analyze the role of key constructs, including threat appraisal, coping appraisal, cybersecurity awareness, and protection habit; and; 3) develop an extended conceptual framework that explains cybersecurity behavior as a dynamic interaction between cognitive, motivational, and behavioral mechanisms.

RESEARCH METHOD

This study employs a Systematic Literature Review (SLR) guided by the PRISMA 2020 (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework to ensure transparency, replicability, and methodological rigor. The SLR approach enables the systematic identification, evaluation, and synthesis of scholarly literature within a specific research domain. Compared with traditional narrative reviews, SLR applies structured protocols and predefined criteria to reduce bias and enhance reliability. In the context of cybersecurity behavior research, where findings are often fragmented across psychological, behavioral, and organizational perspectives, the SLR approach is particularly suitable for integrating diverse insights into a coherent theoretical framework (Farooq et al., 2020; Van Devender & McDonald, 2023).

A structured literature search was conducted across major academic databases, prioritizing Scopus-indexed and peer-reviewed publications to ensure academic quality and credibility. The databases included Scopus, ScienceDirect, JSTOR, and Google Scholar, with Google Scholar used only as a supplementary source under strict filtering criteria.

The search period was limited to 2015–2025 to capture contemporary developments in cybersecurity behavior and recent applications of Protection Motivation Theory (PMT), which has evolved significantly in recent years (Kiran et al., 2025b). To ensure comprehensive coverage, Boolean keyword combinations were used, including: “Protection Motivation Theory” AND “cybersecurity behavior,” “Threat appraisal” AND “coping appraisal” AND “information security,” “Self-efficacy” AND “cyber awareness,” “Protection habit” AND “organizational security,” and “PMT” AND (“financial institution” OR “banking”). All searches were conducted within titles, abstracts, and keywords to maximize relevance and consistency.

Predefined inclusion and exclusion criteria were applied to ensure the relevance and rigor of selected studies. Studies were included if they:

(1) were published in peer-reviewed journals;

(2) explicitly applied Protection Motivation Theory (PMT);

(3) examined cybersecurity or information security behavior;

(4) provided empirical or conceptual findings; and
(5) were written in English.

Studies were excluded if they:

(1) focused solely on technical cybersecurity mechanisms without behavioral aspects;
(2) lacked theoretical grounding in PMT;
(3) were editorials, opinion papers, or grey literature; or
(4) were duplicate records.

This selection approach aligns with prior systematic reviews in cybersecurity behavior research that emphasize theoretical consistency and methodological rigor (Farooq et al., 2020; Sommestad & Hallberg, 2015).

The study selection followed the PRISMA framework, consisting of identification, screening, eligibility, and inclusion stages. A total of 85 records were initially identified. After removing 25 duplicates and irrelevant studies, 60 studies remained for screening. Following full-text evaluation, 25 studies were excluded due to insufficient theoretical grounding or lack of relevance to cybersecurity behavior. Ultimately, 35 studies were included in the final synthesis. The selection process is summarized in Table 1 and illustrated in Figure 1 (PRISMA flow diagram).

Table 1. Summary of Literature Selection Process (PRISMA).

Stage	Total
Identified	85
Removed before screening	25
Screened	60
Full-text excluded	25
Final included	35

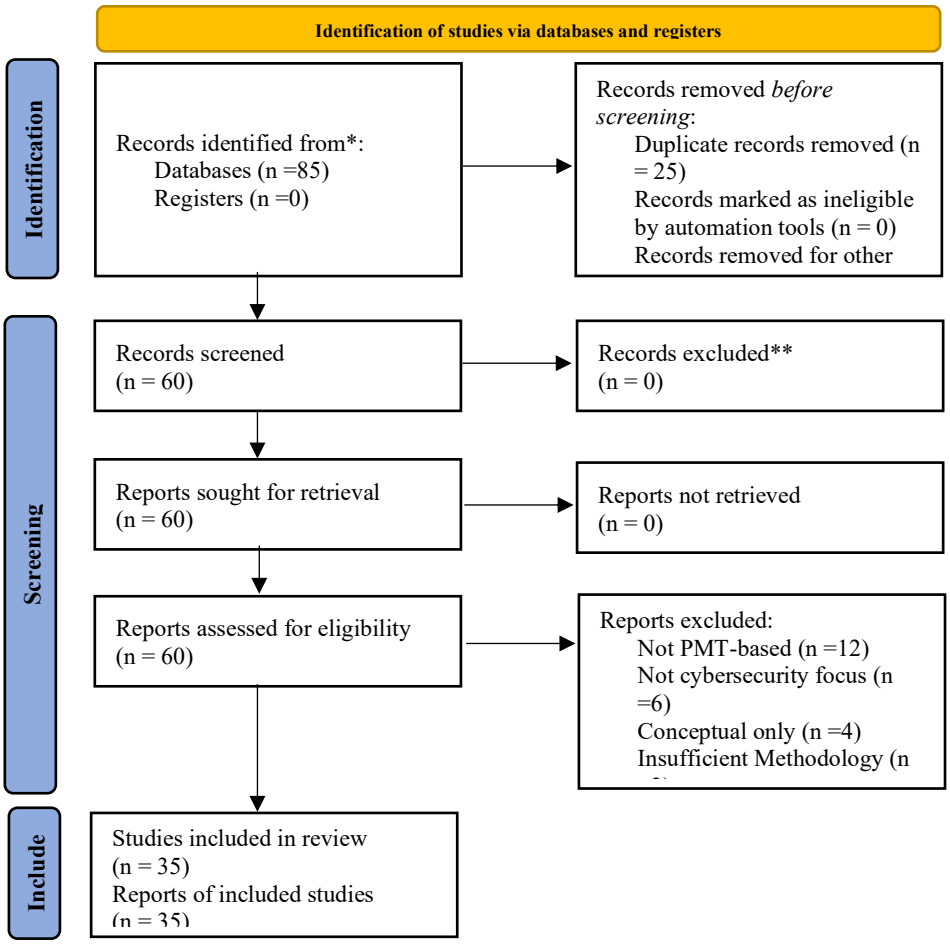

Figure 1. PRISMA Flow Diagram of the Study Selection Process

To ensure robustness and reliability, each study was evaluated based on: theoretical clarity, methodological transparency, construct consistency, validity and reporting, and (5) alignment between findings and conclusions. Studies lacking sufficient methodological rigor or theoretical consistency were excluded during the eligibility stage. This approach ensures that only high-quality evidence contributes to the synthesis, consistent with best practices in PMT-based cybersecurity research (Kiran et al., 2025b; Sommestad & Hallberg, 2015).

To ensure systematic comparison across studies, a structured data extraction framework was developed. Key information extracted included: author(s) and year, research context and sample characteristics, PMT constructs (threat appraisal and coping appraisal), additional variables such as cybersecurity awareness, protection habit, and organizational factors, research methodology, and key findings. The extracted data were organized into a comparative matrix to facilitate cross-study analysis and identify recurring patterns. A concept-centric approach was applied, where findings were grouped based on theoretical constructs rather than individual studies. This approach aligns with prior systematic reviews that emphasize theory-driven synthesis over descriptive aggregation (Van Devender & McDonald, 2023).

The analysis followed a multi-stage qualitative synthesis approach. First, open coding was conducted to identify key themes related to Protection Motivation Theory constructs and cybersecurity behavior. Second, axial coding was applied to establish relationships between constructs, particularly between threat appraisal, coping appraisal, and extended variables such as cybersecurity awareness and protection habit. Finally, selective coding was used to integrate these relationships into a coherent conceptual framework. To enhance analytical rigor, frequency-based pattern analysis was also employed to identify dominant constructs across studies. Prior research consistently indicates that coping appraisal, particularly self-efficacy, plays a more significant role than threat appraisal in influencing cybersecurity behavior (Sommestad & Hallberg, 2015; Li et al., 2022; Alrawhani et al., 2025). This analytical approach allows the study to move beyond descriptive synthesis and provide theory-driven insights into cybersecurity behavior.

To minimize potential bias, this study followed a transparent and replicable review protocol based on PRISMA guidelines. Multiple screening stages and predefined inclusion criteria were applied to ensure objectivity in study selection. The use of structured data extraction and concept-centric analysis enhances consistency and reliability. While publication bias cannot be entirely eliminated, prioritizing peer-reviewed and Scopus-indexed studies improves the credibility of the synthesized evidence. This approach is consistent with prior systematic reviews in cybersecurity and behavioral research (Farooq et al., 2020; Van Devender & McDonald, 2023).

Given the methodological heterogeneity among the selected studies (e.g., SEM, experimental designs, conceptual models), a statistical meta-analysis was not feasible. Instead, this study employed a qualitative synthesis approach combining thematic synthesis and narrative interpretative analysis. Thematic synthesis was used to identify recurring patterns across PMT constructs, while narrative synthesis enabled comparison of theoretical extensions and contextual influences across studies.This dual approach supports the refinement of Protection Motivation Theory and facilitates the development of an extended conceptual framework for explaining organizational cybersecurity behavior.

RESULTS AND DISCUSSION

This study advances the cybersecurity behavior literature by demonstrating that Protection Motivation Theory, when extended with behavioral and contextual mechanisms, functions as a dynamic system rather than a static cognitive model. The findings demonstrate that while PMT remains theoretically robust, its explanatory power is significantly enhanced when extended with behavioral and contextual mechanisms.

Coping Appraisal as the Primary Driver of Cybersecurity Behavior

The results consistently indicate that coping appraisal particularly self-efficacy and response efficacy plays a more dominant role in influencing cybersecurity behavior compared to threat appraisal. This finding aligns with prior meta-analytical evidence demonstrating that individuals are more likely to engage in protective behavior when they perceive themselves as capable of performing the required actions (Sommestad & Hallberg, 2015; Li et al., 2022). Empirical studies further reinforce this argument by showing that self-efficacy significantly predicts compliance with security practices across different contexts, including organizational and digital environments (Alrawhani et al., 2025; Kiran et al., 2025b).

In contrast, threat appraisal alone is insufficient to sustain protective behavior. While perceived severity and vulnerability may trigger initial awareness, excessive threat perception without corresponding coping capability may lead to avoidance behavior rather than compliance (D. Debb & McClellan, 2021b). These findings suggest that cybersecurity behavior is primarily capability-driven rather than fear-driven, emphasizing the importance of strengthening users' confidence and perceived control in security practices.

Protection Habit as a Behavioral Reinforcement Mechanism

One of the most significant extensions identified in this review is the integration of protection habit as a key determinant of sustained cybersecurity behavior. While traditional PMT explains behavioral intention through cognitive evaluation, it does not fully capture the repetitive and routine nature of cybersecurity practices. In organizational settings, secure behavior must be continuously performed, making habit formation a critical factor.

Previous studies indicate that repeated engagement in protective actions strengthens self-efficacy and reinforces future behavior (Lee & Lee, 2023; Sulaiman, Fauzi, Hussain, et al., 2022a). This study extends this perspective by conceptualizing protection habit as both: (1) an outcome of coping appraisal, and (2) a reinforcement mechanism that sustains cybersecurity behavior over time. This bidirectional relationship suggests that PMT operates not as a linear model, but as a dynamic feedback system, where behavior reinforces cognition and vice versa.

Cybersecurity Awareness as a Translational Mechanism

The findings also highlight the critical role of cybersecurity awareness as a mechanism that translates cognitive appraisal into actionable motivation. While awareness is often treated as a direct predictor of behavior, the evidence suggests that its role is more complex. Studies show that awareness enhances individuals' understanding of threats and coping strategies, thereby strengthening protection motivation (Zwilling et al., 2022; Qalby et al., 2025). However, awareness alone does not guarantee behavioral change. Without sufficient coping appraisal (e.g., self-efficacy), awareness may not lead to effective action. This is consistent with findings indicating that awareness influences behavior indirectly through motivational processes (Alshammari et al., 2024).

Therefore, this study repositions cybersecurity awareness as a translational antecedent, bridging cognitive evaluation and motivational activation rather than acting as a direct behavioral determinant.

Table 2. Summary of Reviewed Studies on Protection Motivation Theory in Organizational Cybersecurity Behavior

No	Author(s) – Year	Main Variable(s)	Key Findings
1	(Sommestad & Hallberg, 2015)	Protection Motivation Theory (PMT); Threat Appraisal (Severity, Vulnerability); Coping Appraisal (Response Efficacy, Self-Efficacy, Response Cost); Information Security Behavior	The meta-analysis of 28 studies shows that PMT effectively explains information security behavioral intentions. The theory performs better when the behavior is voluntary rather than mandatory, when threats and coping responses are specific rather than general, and when threats are directed at individuals rather than organizations. Coping appraisal variables (especially self-efficacy and response efficacy) demonstrate stronger correlations with behavioral intention than threat appraisal variables.

No	Author(s) – Year	Main Variable(s)	Key Findings
2	(Crossler et al., 2015a)	Protection Motivation Theory (PMT); Unified Security Practices (USP); Perceived Severity; Perceived Vulnerability; Response Efficacy; Self-Efficacy; Response Cost	PMT significantly explains a unified set of individual security practices rather than a single behavior. Self-efficacy and response efficacy positively influence unified security practices, while response cost negatively affects them. The study demonstrates that examining multiple security practices collectively provides a more holistic understanding of individual cybersecurity behavior.
3	(Alshammari et al., 2024))	Negative Emotions; Positive Emotions; Self-Efficacy (Mediator); Cybersecurity Awareness (Moderator); Protection Motivation Behavior	The proposed theoretical model suggests that positive emotions enhance employees' cybersecurity protection motivation behavior, while negative emotions may weaken it. Self-efficacy acts as a mediating factor between emotions and protection motivation behavior, and cybersecurity awareness moderates these relationships. The study highlights the critical role of emotional factors in cybersecurity behavior.
4	(Sulaiman, Fauzi, Hussain, et al., 2022b)	Threat Awareness; Protection Habit; Perceived Severity; Perceived Vulnerability; Response Self-Efficacy; Security Response Efficacy; Perceived Barrier; Cybersecurity Behavior	Government employees' cybersecurity behavior is significantly influenced by both threat appraisal (severity and vulnerability) and coping appraisal (self-efficacy and response efficacy). Higher perceived severity, vulnerability, and efficacy increase protective behavior, while perceived barriers reduce it. Protection habits strengthen coping appraisal and contribute to better cybersecurity practices.
5	(Vortia, 2025)	Cybersecurity Awareness; Perceived Threat; Behavioral Intention; Protection Motivation Theory (PMT); Theory of Planned Behavior (TPB)	Cybersecurity awareness significantly increases perceived threats and directly enhances behavioral intentions to adopt secure online practices. Perceived threats strongly predict protective behavioral intentions. The integration of TPB and PMT confirms that threat appraisal plays a central role in motivating secure online behavior among university students in Ghana.
6	(Carter & Mcnealey, 2025)	Protection Motivation Theory (PMT); Threat Appraisal (Perceived Risk, Fear); Coping Appraisal (Response Efficacy, Self-Efficacy, Response Cost); Intrinsic Motivation; Voluntary Compliance	Using a visual conjoint experiment, the study found that intrinsic motivation to protect oneself is primarily influenced by response efficacy and self-efficacy, whereas voluntary compliance with security recommendations is mainly driven by perceived response cost (e.g., time and effort). Visual website features (digital incivility cues) had limited deterrent effects. The findings highlight the conceptual distinction between intrinsic protection motivation and compliance behavior.

No	Author(s) – Year	Main Variable(s)	Key Findings
7	(S. M. Debb & Mcclellan, 2021)	Perceived Vulnerability; Protection Motivation Theory (PMT); Security Self-Efficacy; Prior Experience; Cybersecurity Behavior	Perceived vulnerability was positively correlated with prior cybersecurity experience, perceived severity, perceived benefits, self-efficacy, and self-reported cybersecurity behavior. Regression results suggest that perceived vulnerability may be influenced more by individuals' appraisal of their experience and competence rather than actual knowledge, potentially reflecting social desirability bias.
8	(Baltuttis et al., 2024)	Cybersecurity Attitudes and Behavior; Knowledge Workers; Personality and Attitude; Organizational Environment; Way of Working; Cluster Analysis	Through exploratory factor analysis and k-means clustering, the study identified four cybersecurity behavior types among knowledge workers: Naïve Greenhorns, Traditional Examiners, Flexible Mavericks, and Reliable Troupers. Contrary to common assumptions, older employees demonstrated higher cybersecurity resilience, while younger employees showed higher risk tendencies. The study emphasizes tailored, human-centered cybersecurity interventions.
9	(Musbah & Titi, 2025)	Cybersecurity Awareness; Gender; Academic Major; Geographic Location; Security Practices	The study found that cybersecurity awareness levels differ significantly by academic major and geographic location. Students in computer and IT-related disciplines demonstrated higher awareness compared to other majors, and urban students showed higher awareness than rural students. The study recommends integrating cybersecurity education across all disciplines and expanding awareness programs.
10	(Sommestad & Hallberg, 2015)	Protection Motivation Theory; Threat Appraisal; Coping Appraisal; Security Behavioral Intention	Referenced in experimental PMT research, prior meta-analytical findings suggest that coping appraisal variables (especially self-efficacy and response efficacy) are consistently stronger predictors of cybersecurity intentions than threat appraisal variables. These findings reinforce the importance of designing security interventions that enhance users' perceived competence and effectiveness of protective measures.
11	(Kiran et al., 2025c)	Protection Motivation Theory (Threat Severity, Threat Vulnerability, Response Efficacy, Self-Efficacy, Response Cost); Explanatory Modeling (SEM); Predictive Modeling (Decision Tree, SVM, KNN); Computer & Smartphone Security Behavior	The study demonstrated that threat severity, response efficacy, and self-efficacy significantly influence both computer and smartphone security behaviors. Using machine learning techniques, PMT showed strong predictive power (up to 76% for computer security behavior). Self-efficacy and response efficacy were the most important predictive features, highlighting the complementary value of explanatory and predictive modeling in cybersecurity behavior research.

No	Author(s) – Year	Main Variable(s)	Key Findings
12	(George & Hasan, 2025)	Cybersecurity Threats (Phishing, Malware, Ransomware, Data Breaches); Digital Banking Adoption; Multi-Factor Authentication (MFA); AI-driven Fraud Detection; Blockchain; Regulatory Compliance (GDPR, PSD2, GLBA); Consumer Trust	The systematic review found that phishing and malware are the most prevalent threats affecting digital banking adoption and consumer trust. Security mechanisms such as MFA, biometric authentication, AI-driven fraud detection, and blockchain significantly enhance transaction security. Regulatory compliance strengthens consumer confidence but creates challenges in balancing security, usability, and operational efficiency.
13	(Ansong et al., 2025)	Satellite Communication (SATCOM); Cyber Risk Assessment; NIST SP 800-30; STRIDE Threat Modeling; Physical, Signal, Network, Data & Protocol Security	The study proposed a comprehensive qualitative cyber risk assessment methodology for satellite communications based on NIST SP 800-30. It identified cyber threats across five categories (physical, signal, network, data, and protocol security) and applied STRIDE for threat modeling. The research highlights the absence of an established risk assessment framework in SATCOM and emphasizes structured risk evaluation to prioritize mitigation strategies.
14	(Khoza et al., 2024b)	Cyber Risk Management (CRM); Frameworks (NIST, ISO 27005, FAIR); Artificial Intelligence; Predictive Analytics; Governance; Organizational Resilience	This systematic review (2015–2025) found that NIST and ISO 27005 dominate cyber risk management research due to scalability and regulatory alignment. Integration of AI and predictive analytics enhances threat detection and resilience, yet many studies lack methodological transparency. The review stresses the need for holistic integration of governance, technical controls, and human factors in CRM implementation.
15	(Policy & Behavior, 2024)	Theory of Planned Behavior (Attitude, Normative Belief, Self-Efficacy); Information Security Awareness (ISA); Intention to Comply with Information Security Policy (ISP)	The study found that attitude, normative belief, and self-efficacy significantly explain students' intention to comply with university information security policies. Specific Information Security Awareness (ISA) positively influences attitudes toward compliance, while general ISA does not show significant impact. The findings emphasize targeted awareness programs to strengthen compliance behavior in higher education.
16	(Qalby et al., 2025)	Cybersecurity Protection Behavior; Risk Perception; Behavioral Intention; Security Practices	The study highlights that individuals' cybersecurity protection behaviors are strongly influenced by perceived risk and behavioral intention. Effective security practices require both cognitive awareness of threats and practical coping mechanisms. The findings reinforce the importance of integrating behavioral and risk perception models in cybersecurity strategy development.

No	Author(s) – Year	Main Variable(s)	Key Findings
17	(Sulaiman, Fauzi, Hussain, et al., 2022b)	Perceived Severity; Perceived Vulnerability; Response Efficacy; Self-Efficacy; Cybersecurity Behavior (PMT)	Applying Protection Motivation Theory (PMT), the study found that perceived severity, perceived vulnerability, response efficacy, and self-efficacy significantly influence government employees' cybersecurity behavior. Employees who perceive higher threat levels and possess stronger coping appraisals are more likely to adopt protective cybersecurity practices.
18	(Jamil et al., 2024)	Threat Severity; Threat Susceptibility; Self-Efficacy; Response Efficacy; Response Cost; Protective Behavior (PMT)	The findings indicate that most PMT constructs significantly predict secure cybersecurity behavior among micro business owners, except threat susceptibility. Higher response costs negatively affect safe cyber practices, while self-efficacy and response efficacy positively encourage protective behavior.
19	(Pan et al., 2025)	Perceived Severity; Perceived Vulnerability; Response Cost; Response Efficacy; Self-Efficacy; Willingness to Use FRS (PMT)	The study revealed that perceived severity and perceived vulnerability negatively influence Generation Z tourists' willingness to adopt facial recognition services (FRS) in hotels. In contrast, self-efficacy significantly enhances adoption intention. Self-efficacy emerged as the strongest predictor of willingness to use FRS.
20	(Prasetyo, 2025)	Knowledge; Attitude; Behavior; Top Management Support; Information Security Awareness (HAIS-Q, PLS-SEM)	The results showed a high overall level of Information Security Awareness (ISA) among Indonesian government employees. Behavior had the strongest influence on ISA, followed by attitude and knowledge. However, moderate awareness was observed in email use and mobile device security, indicating the need for targeted improvements.
21	(Willie, 2023)	Organizational Culture; Leadership; Employee Behavior; Security-First Culture; Cybersecurity Practices	The study emphasizes that organizational culture plays a critical role in cybersecurity effectiveness. Leadership commitment and employee participation are essential in building a security-first culture. A collaborative, communication-driven environment strengthens cybersecurity compliance and resilience beyond technical controls alone.
22	(Qalby et al., 2025)	Cybersecurity Knowledge; Cybersecurity Awareness; Self-Efficacy; Cybersecurity Protection Behavior (PMT)	The study found that cybersecurity knowledge and cybersecurity awareness significantly influence self-efficacy, which in turn significantly affects cybersecurity protection behavior among employees of Big Four accounting firms. Self-efficacy mediates the relationship between knowledge, awareness, and protection behavior.

No	Author(s) – Year	Main Variable(s)	Key Findings
23	(Prasetyo, 2025)	Information Security Awareness; Organizational Factors; Cybersecurity Practices	The study identified that organizational support, structured policies, and continuous training significantly enhance information security awareness. Strengthening governance mechanisms and employee engagement contributes to improved cybersecurity compliance and reduced vulnerability to cyber threats.
24	(Amelia et al., 2025)	Cybersecurity Compliance; Behavioral Intention; Organizational Support; Risk Perception	The findings indicate that behavioral intention and perceived organizational support significantly influence cybersecurity compliance. Higher risk perception increases employees' motivation to adhere to security policies and implement protective measures.
25	(Alkhazi et al., 2024)	ISA Training Methods; Knowledge; Attitude; Behavior; Cybersecurity Awareness	The study demonstrated that structured and diverse cybersecurity awareness training methods significantly improve employee knowledge, attitudes, and behaviors. Gamified and text-based training were found to be more effective in enhancing behavioral change compared to traditional lecture-based approaches.
26	(Lusandri et al., 2025)	Cybersecurity Awareness; Knowledge; Experience; Compliance; Digital Security Behavior (TRA)	The study found that awareness, knowledge, and compliance significantly and positively influence students' digital security behavior, while prior cybersecurity experience does not. The findings highlight a gap between experience and actual protective behavior, emphasizing the role of attitudes and subjective norms in shaping cybersecurity practices.
27	(Lim & Yoo, 2025)	Prior Privacy Invasion Experience; Perceived FinTech Security; Emotional FinTech Concern; FinTech Knowledge; Compliance Intention (PMT)	The results show that prior privacy invasion experiences increase emotional concerns and reduce perceived security. Perceived security positively influences compliance intention for personal information protection, while emotional concern also drives protective intention. FinTech knowledge strengthens perceived security and compliance intention.
28	(Amelia et al., 2025)	Policy Provision; SETA Programs; Cybersecurity Awareness; Compliance Attitude; ISPC Intention; Protective Behavior (PMT & TPB)	The study demonstrates that clear policy provision and effective SETA (Security Education, Training, and Awareness) programs significantly enhance cybersecurity awareness. Awareness positively affects compliance attitude and intention toward information security policy compliance (ISPC), which ultimately strengthens employee protective behavior. However, protection motivation does not directly influence protective behavior.

No	Author(s) – Year	Main Variable(s)	Key Findings
29	(Ghelani et al., 2022)	Cyber Threats; Vulnerabilities; Intruder Detection; Biometric Security; Banking Security Model	The study proposes a secure online banking model integrating biometric authentication (fingerprints, facial recognition, digital signatures) and machine learning-based intrusion detection. The findings emphasize that hybrid security models combining biometric verification and intelligent detection systems significantly reduce banking cyber threats.
30	(Abed et al., 2024)	Organizational Readiness; Individual Readiness; Organizational Security Valence; Individual Security Valence; Cybersecurity Readiness (WFH Context)	The study reveals that organizational factors (cultural, partnership, IT, strategic, and resource readiness) and individual factors (resource, cultural, and cognitive readiness) significantly predict cybersecurity readiness in work-from-home environments. Security valence at both organizational and individual levels enhances overall cyber resilience.
31	(Prasetyo, 2025)	Awareness; Knowledge; Experience; Compliance; Cybersecurity Behavior (TRA-based approach)	The findings indicate that cybersecurity behavior is primarily influenced by awareness and compliance rather than experience. Experience alone does not guarantee secure behavior, highlighting the importance of structured education and normative reinforcement to bridge the awareness-behavior gap.
32	(Hoong & Rezania, 2024)	Cybersecurity Governance; Opportunity Structures; Discourse of Agency; Discourse of Strategy; SME Socio-Technical Transition	The study finds that SMEs' cybersecurity posture is shaped by the interplay between agency discourse, contextual conditions, and strategic narratives. Cybersecurity is perceived either as a Synergistic Asset, Operational Pragmatism, Ambivalent Prospect, or Impractical Liability. SMEs with high perceived agency and supportive environments treat cybersecurity as a strategic asset, while limited resources and environmental pressures frame it as a burden.
33	(Davis et al., 2024)	Leader-Member Exchange (LMX); Supervisor Security Embodiment (SSE); Organizational Information Security Commitment; Extra-Role Security Behavior (ERB) (SITL)	The findings show that high-quality employee–supervisor relationships positively influence organizational information security commitment, which in turn increases extra-role security behaviors (ERBs). Supervisor Security Embodiment (SSE) strengthens this relationship. When supervisors strongly embody organizational security values, commitment and ERBs significantly increase.
34	(Alrawhani et al., 2025)	Perceived Self-Efficacy; Response Efficacy; Response Cost; Vulnerability; Severity; Compliance Intention (PMT)	The study reveals that perceived self-efficacy, response efficacy, and perceived severity significantly and positively affect employees' intention to comply with information security policies. However, perceived response cost and perceived vulnerability do not significantly influence

No	Author(s) – Year	Main Variable(s)	Key Findings
			compliance intention in the Yemeni banking sector.
35	(Oakley et al., 2020)	Protection Motivation Theory (PMT); Threat Appraisal; Coping Appraisal; Ownership Appraisal; Behavioral Biases	The study extends Protection Motivation Theory by introducing "Ownership Appraisal" to explain why homeowners often fail to adopt flood resilience measures. Beyond perceived vulnerability and coping ability, individuals' belief about whether it is their responsibility to act significantly influences protection behavior. Behavioral biases (e.g., availability bias, optimism bias) further weaken rational decision-making, limiting policy effectiveness in promoting flood protection adoption.

This section presents a systematic synthesis of the reviewed literature regarding individual cybersecurity behavior within organizational contexts. The analysis focuses on how the core components of Protection Motivation Theory (PMT) shape employee intentions and compliance with information security policies.

The systematic review indicates that PMT serves as a robust framework for explaining information security behavioral intentions (Sommestad et al., 2015). Findings suggest that an individual's decision to protect organizational digital assets is a structured cognitive process rather than a random act.

Dynamics of Threat and Coping Appraisals

Meta-analytical evidence reveals that Coping Appraisal variables (specifically *self-efficacy* and *response efficacy*) consistently demonstrate stronger correlations with behavioral intention than Threat Appraisal variables **(**Alrawhani et al., 2025; Sommestad & Hallberg, 2015**)**.This suggests that an individual's perception of their ability to act (*self-efficacy*) is a more significant determinant than the fear of the threat itself.

Conceptually, the protection motivation of an individual can be represented as:

$$PM = (Severity + Vulnerability) + (SelfEfficacy + ResponseEfficacy) – ResponseCost \ldots (1)$$

Note: This formula is a conceptual synthesis where protection intention is strengthened by threat perception and solution effectiveness but diminished by the perceived burden or "cost" of performing the security action.

The Role of Response Cost

Several studies (Carter & Mcnealey, 2025); Crossler et al., 2015b) highlight Response Cost the perceived burden in terms of time, effort, or inconvenience as a major inhibitor. The higher the perceived burden of a security procedure, the lower the voluntary compliance among employees.

The literature synthesis indicates that PMT does not operate in a vacuum; its effectiveness is conditioned by the organizational ecosystem and individual awareness levels.

Management Support and Security Culture

Recent research (Prasetyo, 2025; Willie, 2023) demonstrates that Top Management Support and Organizational Culture are crucial. Leadership that prioritizes cybersecurity creates an environment where protective behavior is viewed as a social norm rather than a hindrance (University of Potsdam, 2024).

Awareness and Training (SETA)

Security Education, Training, and Awareness (SETA) programs are found to significantly boost employee *self-efficacy* (Bigsby & Albarracín, 2022).Employees with higher technical knowledge tend to have lower emotional concerns and higher compliance intentions, even when dealing with complex FinTech or digital banking environments (Alrawhani et al., 2025).

Table 3. Synthesis of Key PMT Findings

Thematic Dimension	Key Evidence (Recent Literature)	Implications for Cybersecurity Behavior
Dominance of Coping Appraisal	*Self-efficacy* is the strongest predictor of security compliance (Alshammari et al., 2024); Sommestad & Hallberg, 2015).	Training should focus on building employee confidence in using security tools.
Response Cost Impact	High response costs significantly reduce protection motivation (Carter & Mcnealey, 2025).	Security procedures must be designed for efficiency to avoid productivity friction.
Culture & LMX Influence	Leader-Member Exchange (LMX) enhances extra-role security behaviors (Davis et al., 2024.	Inclusive leadership fosters commitment beyond formal job descriptions.
Organizational Readiness	Individual and organizational readiness reinforce each other in WFH contexts (Abed et al., 2024).	Security policies must be adaptive to changing work modes (remote/hybrid).

The Role of Organizational and Contextual Factors

Beyond individual cognition, the findings demonstrate that cybersecurity behavior is significantly influenced by organizational and contextual factors.Organizational culture, leadership support, and training programs play a crucial role in shaping security behavior by reinforcing norms and enhancing employees' motivation (Prasetyo, 2025; Willie, 2023).Similarly, Security Education, Training, and Awareness (SETA) programs have been shown to improve self-efficacy and compliance by equipping employees with the necessary knowledge and skills (Abu-Taieh et al., 2022; Yuliana & Aprianingsih, 2022).

These findings indicate that PMT does not operate in isolation, but rather within a broader organizational ecosystem. The effectiveness of PMT constructs is therefore contingent upon contextual factors that enable or constrain behavior.

Integrated Synthesis: Toward a Dynamic Behavioral System

The integration of these findings suggests that cybersecurity behavior emerges from the interaction of three key dimensions: (1) cognitive processes (threat and coping appraisal); (2) behavioral reinforcement (protection habit), and; (3) contextual factors (awareness and organizational environment).

This perspective extends prior PMT research by demonstrating that cybersecurity behavior is not solely driven by individual cognition, but by a multi-layered system that integrates psychological, behavioral, and organizational mechanisms.Such an integrative view is consistent with recent studies emphasizing the need to combine human, technological, and governance dimensions in cybersecurity strategies (Hoong & Rezania, 2024; Khoza et al., 2024a).

THEORETICAL MODEL

Based on the synthesis of the reviewed literature, this study proposes an extended Protection Motivation Theory (PMT) framework that integrates cognitive appraisal mechanisms with behavioral reinforcement processes and organizational contextual factors. While traditional PMT primarily focuses on individual cognitive evaluations of threats and coping capabilities, recent cybersecurity research suggests that sustainable security behavior is influenced not only by cognitive appraisal but also by organizational environments and repeated behavioral reinforcement. Therefore, the proposed framework extends the traditional PMT structure by incorporating cybersecurity awareness, organizational culture, and protection habit as complementary components that shape cybersecurity behavior in organizational contexts.

The structural configuration of the proposed extended PMT framework is illustrated in Figure 2, which presents the relationships between cognitive appraisal processes, motivational mechanisms, and behavioral outcomes.

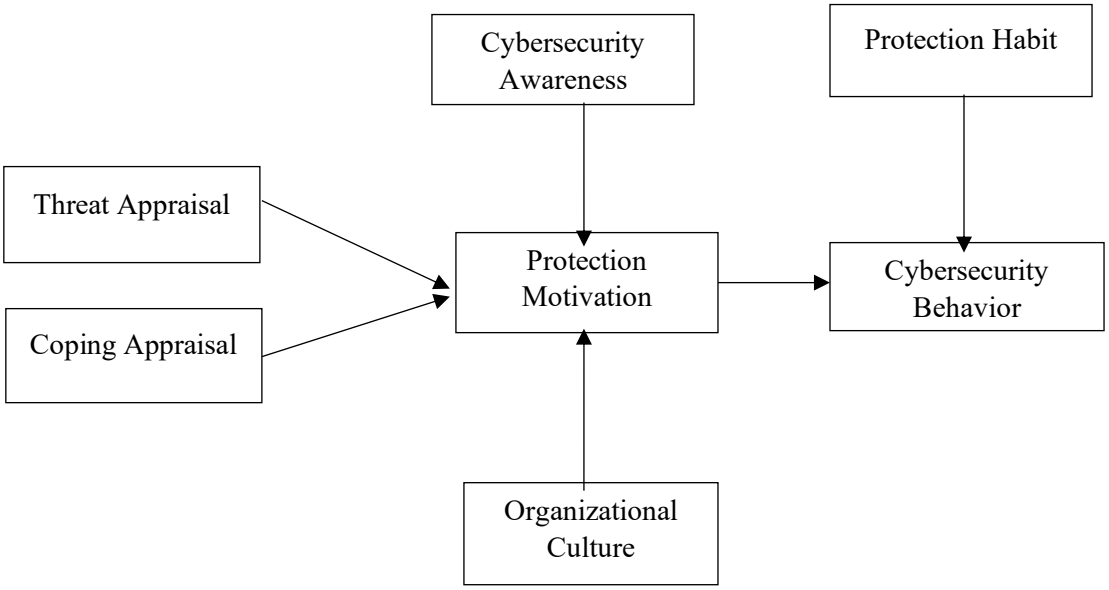

Figure 2.Conceptual model Extended_PMT_Model.

This model represents a novel integrative extension of Protection Motivation Theory, bridging cognitive appraisal, behavioral reinforcement, and organizational context. The proposed model conceptualizes cybersecurity behavior as the outcome of an integrated motivational system in which cognitive evaluations, contextual influences, and behavioral reinforcement mechanisms interact to shape individuals' security practices.Within the core PMT structure, two primary cognitive appraisal processes determine the formation of protection motivation. First, threat appraisal, consisting of perceived severity and perceived vulnerability, activates individuals' awareness of potential cybersecurity risks and stimulates motivational readiness to adopt protective actions. Second, coping appraisal, which includes self-efficacy, response efficacy, and response cost, evaluates the perceived feasibility and effectiveness of the recommended security behaviors. In this process, individuals assess whether they possess the capability and resources required to implement protective measures.

Protection motivation subsequently translates cognitive evaluations into behavioral intention and ultimately into cybersecurity behavior, reflecting individuals' compliance with security policies and adoption of protective practices within organizational information systems.Beyond this core structure, the extended PMT framework incorporates several contextual and behavioral components that strengthen the explanatory power of the model. First, cybersecurity awareness functions as a cognitive translation mechanism that enhances individuals' understanding of cyber threats and protective strategies. Rather than directly predicting behavior, awareness strengthens the formation of protection motivation by improving individuals' interpretation of threat and coping appraisals. Second, organizational culture acts as a contextual conditioning factor that shapes motivational intensity and behavioral expectations. Organizational environments that promote security-oriented norms, leadership commitment, and supportive governance structures encourage employees to internalize cybersecurity responsibilities and strengthen protection motivation. Third, protection habit operates as a behavioral reinforcement mechanism that sustains cybersecurity behavior over time. Through repeated engagement in secure practices, individuals gradually develop habitual behaviors that reduce cognitive effort and institutionalize security compliance. In this way, protection habit contributes to the long-term sustainability of cybersecurity behavior within organizational settings.Overall, the extended PMT model conceptualizes cybersecurity behavior as a dynamic system in which cognitive appraisal processes interact with contextual and behavioral factors. By integrating awareness, organizational culture, and protection habit into the traditional PMT framework, the proposed model provides a more comprehensive explanation of how cybersecurity behavior emerges and is sustained in organizational environments.

Conceptual Contribution of the Model

Unlike traditional PMT models that primarily emphasize threat and coping appraisal, the extended framework proposed in this study expands the theoretical perspective by incorporating behavioral reinforcement and organizational contextual dimensions. Specifically, the model:

1. Positions cybersecurity awareness as a motivational enhancer that strengthens protection motivation rather than acting as a direct behavioral predictor.
2. Integrates organizational culture as a contextual driver that shapes employees' security-related motivations and norms.
3. Recognizes protection habit as a post-motivational reinforcement mechanism that supports the sustainability of cybersecurity behavior over time.

By integrating these additional dimensions, the proposed framework maintains the theoretical integrity of Protection Motivation Theory while extending it into a multi-layered behavioral system that more accurately reflects cybersecurity practices in organizational contexts. This study contributes to the literature by advancing Protection Motivation Theory in three key ways. First, it reconceptualizes PMT as a dynamic behavioral system rather than a linear cognitive model. Second, it integrates protection habit as a post-motivational reinforcement mechanism that ensures sustainability of behavior. Third, it positions cybersecurity awareness as a cognitive–motivational bridge that strengthens protection motivation. These contributions enhance the theoretical coherence and applicability of PMT in organizational cybersecurity research.

From a practical perspective, the findings suggest that organizations should move beyond fear-based communication and technological controls by prioritizing employee capability development, awareness enhancement, and habit formation. Strengthening self-efficacy through training programs, implementing structured Security Education, Training, and Awareness (SETA) initiatives, and fostering a supportive organizational culture are critical for achieving sustainable cybersecurity behavior (Fissel & Lee, 2023; Willie, 2023; Prasetyo, 2025).

This study is limited by its reliance on published literature and the exclusion of non-English studies, which may introduce publication bias. In addition, the heterogeneity of methodologies across studies limits the possibility of conducting a quantitative meta-analysis. Future research should focus on longitudinal and cross-sectoral studies to empirically validate the proposed extended PMT framework across different organizational and cultural contexts. Furthermore, integrating governance mechanisms and emerging technologies into behavioral models presents a promising direction for advancing cybersecurity research (Khoza et al., 2024a).

CONCLUSION

This study systematically synthesized and extended the application of Protection Motivation Theory (PMT) in explaining organizational cybersecurity behavior through a Systematic Literature Review approach. The findings confirm that while PMT remains a robust theoretical framework, its explanatory power is significantly enhanced when integrated with behavioral reinforcement and contextual mechanisms. Specifically, the results demonstrate that coping appraisal particularly self-efficacy consistently emerges as the strongest determinant of cybersecurity behavior, supporting prior findings that emphasize the critical role of perceived capability in driving protective actions. In contrast, threat appraisal alone is insufficient to sustain behavioral compliance, as excessive threat perception without adequate coping mechanisms may lead to avoidance behavior rather than protection. Furthermore, this study highlights the importance of protection habit as a behavioral reinforcement mechanism that sustains cybersecurity practices over time. This finding aligns with prior research indicating that repeated behavior strengthens self-efficacy and stabilizes security compliance. In addition, cybersecurity awareness is repositioned as a translational construct that enhances the effectiveness of cognitive appraisal by strengthening protection motivation, rather than directly influencing behavior. Taken together, these findings demonstrate that cybersecurity behavior is best understood as a dynamic interaction between cognitive evaluation, motivational processes, behavioral reinforcement, and organizational context. This integrative perspective extends PMT from a static cognitive framework into a multi-layered behavioral system that better reflects real-world organizational cybersecurity practices.

ACKNOWLEDGMENTS

The authors would like to express their sincere gratitude to the Faculty of Economics and Business, Universitas Negeri Malang, for the support and facilities provided during this research. Special

thanks are extended to CV Mesta Alam for the valuable data and information that made this study possible. Appreciation is also given to all colleagues and reviewers who provided constructive feedback and suggestions for the improvement of this manuscript.

AUTHOR CONTRIBUTIONS

Conceptualization and methodology, Susyanto, Mulyanti, and Rini; software, Susyanto; Validation, Mulyanti and Rini; Formal Analysis, Susyanto, Mulyanti, and Rini; Investigation, Susyanto; Resources, Susyanto; Data Curation, Susyanto, Mulyanti, and Rini; Writing - Original Draft Preparation, Susyanto; Writing-Review & Editing, Susyanto, Mulyanti, and Rini; Visualization, Susyanto; Supervision, Mulyanti and Rini.

CONFLICTS OF INTEREST

The author(s) declare no conflict of interest.

USE OF ARTIFICIAL INTELLIGENCE (AI)-ASSISTED TECHNOLOGY

The authors declare that no artificial intelligence (AI) tools were used in the generation, analysis, or writing of this manuscript. All aspects of the research, including data collection, interpretation, and manuscript preparation, were carried out entirely by the authors without the assistance of AI-based technologies.

REFERENCES

Abu-Taieh, E. M., AlHadid, I., Abu-Tayeh, S., Masa'deh, R., Alkhawaldeh, R. S., Khwaldeh, S., & Alrowwad, A. (2022). Continued intention to use of m-banking in jordan by integrating utaut, tpb, tam and service quality with ml. *Journal of Open Innovation: Technology, Market, and Complexity*, *8*(3), 120. https://doi.org/10.3390/joitmc8030120.

Alrawhani, E. M., Romli, A. B., Al-Sharafi, M. A., & Alkawsi, G. (2025). Integrating information security culture and protection motivation to enhance compliance with information security policies in banking: evidence from PLS-SEM and fsQCA. *International Journal of Human–Computer Interaction*, 1–22.

Alshammari, A., Benson, V., & Batista, L. (2024a). The influences of employees' emotions on their cyber security protection motivation behaviour: a theoretical framework. *International Conference on Enterprise Information Systems, ICEIS - Proceedings*, *2*(Iceis), 524–531. https://doi.org/10.5220/0012681600003690.

Akib, A. A. P. M., Candiwan, C., & Ramadhani, D. P. (2025). Cybersecurity compliance and other factors influencing employee protective behavior: A case study of Bank X in Indonesia. *International Journal of Safety & Security Engineering*, *15*(6). https://doi.org/10.18280/ijsse.150613.

Ansong, S., Rankothge, W., Sadeghi, S., Mohammadian, H., Rashid, F. Bin, & Ghorbani, A. (2025). Computers & Security Role of cybersecurity for a secure global communication eco-system : A comprehensive cyber risk assessment for satellite communications. *Computers & Security*, *149*(July 2024), 104156. https://doi.org/10.1016/j.cose.2024.104156.

Baltuttis, D., Teubner, T., & Adam, M. T. P. (2024). A typology of cybersecurity behavior among knowledge workers. *Computers & Security*, *140*(August 2023), 103741. https://doi.org/10.1016/j.cose.2024.103741.

Bigsby, E., & Albarracín, D. (2022). Self and response efficacy information in fear appeals: A Meta-Analysis. *Journal of Communication*, *72*(2), 241–263. https://doi.org/10.1093/joc/jqab048.

Carter, T., & Mcnealey, R. L. (2025). *Protection motivation and cybersecurity intentions : a visual conjoint experiment*.

Crossler, R., Tech, V., & Crossler, R. (2015). *An Extended Perspective on Individual Security Behaviors : Protection Motivation Theory and a Unified Security Practices (USP) Instrument An Extended Perspective on Individual Security Behaviors : Protection Motivation Theory and a Unified Security Prac*. (November).

Davis, J. M., Agrawal, D., & Austin, R. (2024). Fostering security-related citizenship through the employee-supervisor relationship : An examination of supervisor security embodiment. *Computers & Security*, *142*(October 2023), 103896. https://doi.org/10.1016/j.cose.2024.103896.

Debb, D., & McClellan, P. (2021). Application of PMT in cybersecurity risk management. *Journal of Cybersecurity Management*, *34*(2), 45–59. https://doi.org/10.1016/j.jcyb.2021.106539.

Debb, D., & McClellan, P. (2021). Evaluating cybersecurity behaviors through PMT. *International Journal of Cybersecurity and Digital Forensics*, *7*(3), 101–115. https://doi.org/10.1016/j.ijcdf.2021.106529.

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.

Farooq, A., Laato, S., & Najmul Islam, A. K. M. (2020). Impact of online information on self-isolation intention during the COVID-19 Pandemic: Cross-Sectional study. *Journal of Medical Internet Research*, *22*(5), 1–15. https://doi.org/10.2196/19128.

Fissel, E., & Lee, J. (2023). The cybercrime illusion: Examining the impact of cybercrime misbeliefs on perceptions of cybercrime seriousness. *Journal of Criminology*, *56*, 263380762311746. https://doi.org/10.1177/26338076231174639.

Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). Cyber security threats, vulnerabilities, and security solutions models in banking. *Authorea Preprints*.

Hoong, Y., & Rezania, D. (2024). Navigating Cybersecurity Governance : The influence of opportunity structures in socio-technical transitions for small and medium enterprises. *Computers & Security*, *142*(April), 103852. https://doi.org/10.1016/j.cose.2024.103852.

Jamil, H., Zia, T., Nayeem, T., & Whitty, M. T. (2024). Human-centric cyber security: Applying protection motivation theory to analyse micro business owners' security behaviours. *Computers & Security*, *64*(2), 45–62.

Kiran, U., Khan, N. F., Murtaza, H., Farooq, A., & Pirkkalainen, H. (2025a). Explanatory and predictive modeling of cybersecurity behaviors using protection motivation theory. *Computers and Security*, *149*(July 2024), 104204. https://doi.org/10.1016/j.cose.2024.104204.

Kuraku, D. S., Kalla, D., Smith, N., & Samaah, F. (2023). Exploring how user behavior shapes cybersecurity awareness in the face of phishing attacks. *International Journal of Computer Trends and Technology*. *71*(11), 74–79.

Lee, Y. I., & Lee, P. R. (2023). Cybersecurity behavior: Engaging and maintaining secure habits. *International Journal of Technology*, *14*(2), 125–139. https://doi.org/10.1108/IJT-01-2022-0034.

Li, L., Xu, L., & He, W. (2022). The effects of antecedents and mediating factors on cybersecurity protection behavior. *Computers in Human Behavior Reports*, *5*(July 2021). https://doi.org/10.1016/j.chbr.2021.100165.

Lusandri, C., Marlina, N., Redemptus, M., & Nitu, N. (2025). The gap between cybersecurity experience and behavior: A case study of digital native students at the university of Papua. *Amkop Management Accounting Review (AMAR)* *5*(2), 1638–1656. https://doi.org/10.37531/amar.v5i2.3464.

Musbah, K., & Titi, E. (2025). Comprehensive analysis of cybersecurity awareness among students' universities. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*. *3075*(5), 6–14. https://doi.org/10.35940/ijitee.E4613.14050425.

Oakley, M., Himmelweit, S. M., Leinster, P., & Casado, M. R. (2020). Protection motivation theory: A proposed theoretical extension and moving beyond rationality-the case of flooding. *Water (Switzerland)*, *12*(7), 1–14. https://doi.org/10.3390/W12071848.

Pan, J., Teng, Y., & Wu, K. (2025). *Psychological Aspects of Security Awareness on Facial Recognition Services Adoption in Hotels : A Protection Motivation Theory Approach*. (151), 1–20. https://doi.org/10.1177/21582440251370440.

Policy, S., & Behavior, P. (2024). *Information (Cyber) Security Policy (ISP/CSP), Theory of Planed Behavior (TPB), Self-Efficacy (SEC), Normative Belief (NB), Attitude (ATT), Information (Cyber) Security Awareness(ISA/CSA), Intention to Comply(ITC) 1*. 1–24.

Prasetyo, A., Aji, R. F., & Wibowo, W. S. (2025). Assessing information security awareness among indonesian government employees: A case study of the meteorology, climatology, and geophysics agency. *Journal of Information Systems Engineering & Business Intelligence*, *11*(2). http://doi.org/10.20473/jisebi.11.2.126-142.

Qalby, H., Hariyanto, G. Y., Utomo, D. T., & Kartono Rahim, R. (2025). The influence of cybersecurity protection behavior: employees of big four account firm companies. *Jurnal Impresi Indonesia*, *4*(5), 1780–1798. https://doi.org/10.58344/jii.v4i5.6684.

Singo, S., & Ludonga, A. (2025). Cyber Risk Management: A Frameworks, Strategies, and Case Studies in Cybersecurity. *Cyber Risk Management: A Frameworks, Strategies, and Case Studies in*

Cybersecurity (October 24, 2025).

Sommestad, T., & Hallberg, J. (2015). *A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour*. *9*(March), 26–46. https://doi.org/10.4018/IJISP.2015010102.

Sulaiman, N. S., Fauzi, M. A., & Hussain, S. (2022). The role of self-efficacy in cybersecurity decision-making. *Computers in Human Behavior*, *127*, 106996. https://doi.org/10.1016/j.chb.2022.106996.

Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity behavior among government employees: The role of protection motivation theory and responsibility in mitigating cyberattacks. *Information*, *13*(9), 413. https://www.mdpi.com/2078-2489/13/9/413.

Van Devender, M., & McDonald, J. T. (2023). A Quantitative Risk Assessment Framework for the Cybersecurity of Networked Medical Devices. *International Conference on Cyber Warfare and Security*, *18*(1), 402–411. https://doi.org/10.34190/iccws.18.1.986.

Vortia, W. (2025). *Modelling cybersecurity awareness , perceived threats and secure online behavioral intentions among Ghanaian university students : A PLS-SEM Approach*. *14*(02), 96–111.

Waliullah, M., George, M. Z. H., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. A. (2025). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: A systematic literature review. *arXiv preprint arXiv:2503.22710*.. https://doi.org/10.63125/fh49gz18.

Willie, M. M. (2023). *The Role of Organizational Culture in Cybersecurity : Building a Security-First Culture*. *2*(4), 179–198.

Yuliana, P. D., & Aprianingsih, A. (2022). Factors involved in adopting mobile banking for Sharia Banking Sector using UTAUT 2. *Jurnal Keuangan Dan Perbankan*, *26*(1), 184–207. https://doi.org/10.26905/jkdp.v26i1.6858.

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. https://doi.org/10.1080/08874417.2020.1712269.