Asia-Pacific Journal of Information Technology and Multimedia 15(1) 2026: 362 – 378
https://doi.org/10.17576/apjitm-2026-1501-23

Cybersecurity Awareness and Behaviour Theory Models: A Systematic Literature Review

Kesedaran Keselamatan Siber dan Model Teori Tingkah Laku: Satu Tinjauan Literatur Sistematik

Nor 'Afifah Binti Sabri[*1], *Aun Yichiet*[1], *Gan Ming Lee*[1],
William Yeoh Ging Sun[2], *Lee-Kwun Chan*[1]

[1]*Faculty of Information and Communication Technology,*
Universiti Tunku Abdul Rahman, Malaysia

[2]*Lee Shau Kee School of Business and Administration,*
Hong Kong Metropolitan, University, Hong Kong

[*]*Corresponding author: afifahs@utar.edu.my*

Received 25 November 2025
Accepted 28 April 2026, Available online 30 June 2026

ABSTRACT

Security behaviour models serve as foundational frameworks for studying human behaviour in the context of information security. Previous research has used various type of security behaviour models and cybersecurity awareness theories to better understand people's security-related behaviours. This paper presents a systematic literature review (SLR) of human security behaviour models and theories applied in cybersecurity research over the past five years (2020-2025). Using a structured four-phase SLR methodology that includes planning, source selection, information gathering, and analysis, a total of 173 publications were methodically chosen from five major academic databases: Science Direct, IEEE Xplore, ACM Digital Library, Research Gate, and Google Scholar. From the analysis, 54 distinct behavioural theories were identified, of which five were most frequently applied: The Theory of Planned Behaviour (TPB), Theory of Reasoned Action (TRA), Protection Motivation Theory (PMT), Fogg Behaviour Model (FBM) and Knowledge-Attitude-Behaviour (KAB) Model. Every model is thoroughly investigated in terms of its theoretical fundamentals, components, and practical applications in cybersecurity. The findings of the literature will provide a form of integrated theoretical map that might assist practitioners and academicians in adopting appropriate behavioural models for cybersecurity approaches. These findings will be applied to develop a conceptual model for a future study on how cybersecurity influences human behaviour in Malaysian Small and Medium-sized Enterprises (SMEs).

Keywords**:** Cybersecurity; Human Behaviour Model; Information Security; Security Behaviour Model; Systematic Literature Review

ABSTRAK

Model tingkah laku keselamatan berfungsi sebagai kerangka asas bagi mengkaji tingkah laku manusia dalam konteks keselamatan maklumat. Kajian-kajian terdahulu telah menerapkan pelbagai model dan teori tingkah laku keselamatan yang berkaitan dengan kesedaran keselamatan siber untuk memahami tindakan individu yang berkaitan dengan keselamatan. Manuskrip ini membentangkan tinjauan literatur sistematik (SLR) mengenai model dan teori tingkah laku keselamatan manusia yang telah diterapkan dalam penyelidikan siber sepanjang lima tahun yang lalu (2020-2025). Sebanyak 173 penerbitan telah dipilih secare sistematik daripada lima pengkalan data akademik utama iaitu Science Direct, IEEE Xplore, ACM Digital Library, ResearchGate, dan Google Scholar dengan menggunakan metodologi SLR empat fasa yang berstruktur merangkumi perancangan, pemilihan sumber, pengumpulan maklumat, dan analisis. Daripada analisis tersebut, 54 teori tingkah laku yang berbeza telah dikenal pasti, dengan lima daripadanya yang paling kerap digunakan: Teori Tingkah Laku Terancang (TPB), Teori Tindakan Beralasan (TRA), Teori Motivasi Perlindungan (PMT) Model Tingkah-Laku Fogg, dan Model Pengetahuan-Sikap-Tingkah Laku. Setiap model diperiksa secara kritis dari segi asas teori, elemen konstituen, aplikasi empirikal dalam konteks keselamatan siber, serta kekuatan dan batasan masing-masing. Penemuan ini menyediakan peta teori yang bersepadu bagi membimbing penyelidik dan pengamal dalam memilih model tingkah laku yang sesuai untuk intervensi keselamatan siber. Hasil daripada tinjauan ini akan memaklumkan pembangunan model konseptual bagi penyelidikan empirikal masa hadapan dalam membentuk tingkah laku keselamatan di kalangan Perusahaan Kecil dan Sederhana (PKS) di Malaysia.

Kata kunci**:** Keselamatan Siber, Model Tingkah-Laku Manusia, Keselamatan Maklumat, Model Tingkah-Laku Keselamatan, Tinjauan Literatur Sistematik

INTRODUCTION

In global information security environments, human behaviour is one of the most common and risky security vulnerabilities (Arend et al., 2020). The common pattern can be seen in most previous research studies where a lot of cybersecurity incidents do not happen because of purely technical failures but rather because of human error, simple negligence, or being too easily manipulated by social engineering attack (Meshkat et al., 2020). Furthermore, it is critical to understand the models that effectively influence human security behaviour because cyber attackers tend to use psychological and behavioural weaknesses to advance their cyber-attacks (Sulaiman et al., 2022)

A key insight from the research is that awareness doesn’t really lead to secure behaviour. Awareness alone is insufficient to ensure system security, where human behaviour remains a critical determinant of cybersecurity resilience (Lin & Luo, 2021). Even with high level of cyber security expertise, people may still do risky behaviour (Alsharida et al., 2023). This awareness-behaviour gap implies that cognitive issues, social pressures, and motivational drivers should be handled all at once, through interventions that are firmly based on theory (Chaudary, 2024). In organisational contexts, cultivating a 'human firewall' where each individual act as a proactive defence mechanism requires a comprehensive understanding of the psychological determinants of security behaviour (Triplett, 2022; Tikanmäki & Ruoslahti, 2024).

Information security behaviour model studies typically consist of five main goals: (1) assessing people’s current security behaviour; (2) forecasting future security behaviour intentions; (3)

encouraging the continuation of secure practices; (4) encouraging the adoption of protective behaviours; and (5) influencing behavioural change. This taxonomy of purposes underscores the breadth of applications for which behaviour models are employed.
Despite extensive application of behavioural theories in the cybersecurity literature, a consolidated and up-to-date synthesis of the most widely used models, their theoretical origins, core components, and empirical evidence base remains limited. In order to close this gap, this study does a systematic literature review (SLR) in order to determine, evaluate, and synthesise the most frequent human security behaviour models used in cybersecurity research between 2020 and 2025.

The structure of the rest of this article is as follows: an overview of human behaviour in cybersecurity is provided in Section 2; the research methodology is presented in Section 3; the five main behaviour models are assessed in section 4; the results are discussed in Section 5; and the research and practical implications are concluded in Section 6.

OVERVIEW OF HUMAN BEHAVIOUR IN CYBERSECURITY

The efficacy of any security system is ultimately dictated by the actions of its human users, event though the technical measures like firewalls, intrusion detection systems, and encryption protocols are essential to cybersecurity (Lin & Luo, 2021). The widely used cybersecurity axiom that "humans are the weakest link" reflects the understanding that human error, negligence or intentional policy breaches can compromise even the most technically advanced system (Alkhazi et al., 2022; Sangwan, 2024). A simple act such as an employee unknowingly downloading malware-infected files or sharing credentials with an unauthorised party can render sophisticated technical protections ineffective. Therefore, it is crucial to understand and influence human behaviour because people are not just technology users but also proactive participants who serve as the first line of defense in any security framework (Tikanmäki & Ruoslahti, 2024). This section analyzes the main behavioural potential risks resulting from user behaviours, defines important theoretical concepts, and examines at how human behaviour affects cybersecurity.

Human behaviour in the context of cybersecurity includes people's obvious behaviours, attitudes, and cognitive processes that impact information systems' level of security. This domain revolves around two fundamental concepts. First, an individual's level of knowledge and comprehension of risks, vulnerabilities, and the safeguards available within an organization's information environment is referred to as information security awareness. Second, an individual's specific behaviours or inactions in reaction to security policies, training, and threats are referred to as information security behaviour (Yeoh et al., 2023)

The relationship between awareness and behaviour is not linear. Research has demonstrated that awareness is a necessary but insufficient precondition for secure behaviour (Chaudhary, 2024). Social norms, self-efficacy, perceived ease of compliance, and the presence of enabling triggers collectively mediate the translation of awareness into action. The primary contribution of behavioural theory to cybersecurity research is an understanding of these mediating elements, which effectively explain how behaviour lies between actions and consequences.

A successful security strategy should not only include technical measures but also staff training programs, policy enforcement mechanisms, and the culture of security awareness within the organisation (Yeoh et al., 2022). This paper focuses specifically on the theoretical behaviour

models that provide the conceptual scaffolding for such human-centric cybersecurity interventions.

METHODOLOGY

This research study employed a Systematic Literature Review (SLR) approach to gather and synthesise published research with peer-reviewed on human security behaviour models and how they are applied in cybersecurity. The SLR process was designed in four sequential phases: (1) Planning phase, (2) Sources Selection phase, (3) Information Gathering phase, and (4) Analysis phase. This structured approach ensures transparency, replicability, and thoroughness in evidence synthesis (Kitchenham & Charters, 2007). The overall SLR workflow illustrates in Figure 1.

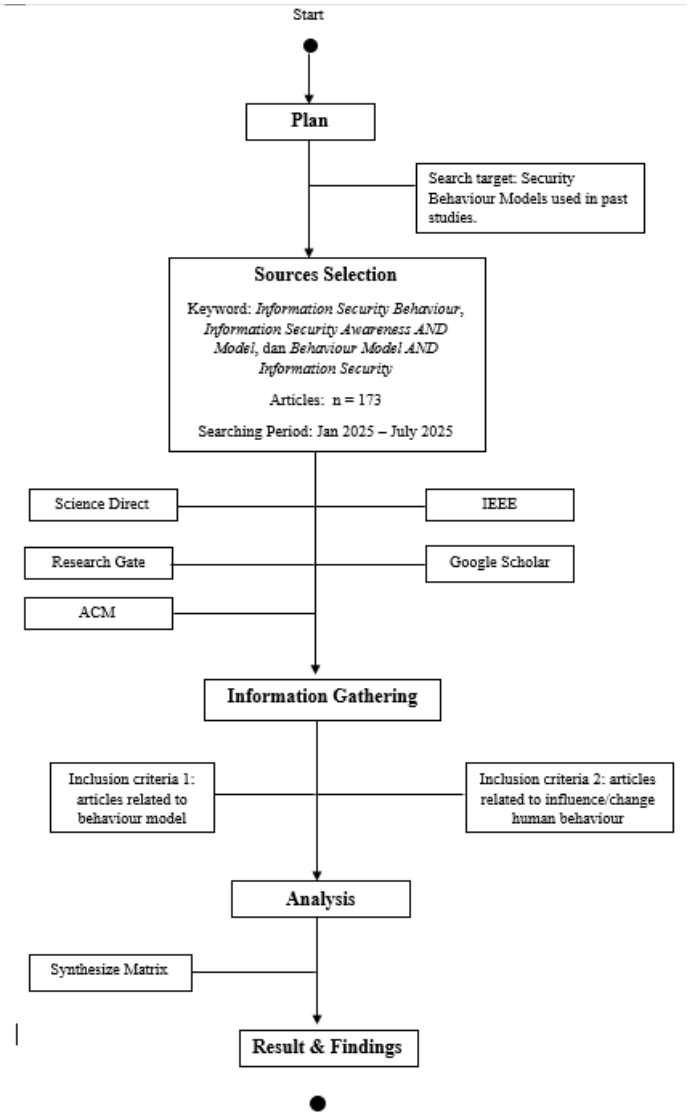

FIGURE 1. Systematic Literature Review – Flow

PLANNING PHASE

The goal and scope of the study were established at the planning phase, prior to the beginning of data collection. The purpose of this research study is to determine and investigate the

security behaviour models that are most frequently used in empirical investigations of human information security behaviour. In this research study, a systematic review method has been chosen.

SOURCE SELECTION PHASE

Science Direct, IEEE Xplore, ACM Digital Library, Research Gate, and Google Scholar are the five main online academic databases from which publications were sourced during the sources selection process. The string-keyword used in the searching process were: (1) “Information Security Behaviour”; (2) “Information Security Awareness” AND “Model”; (3) “Behaviour Model” AND “Information Security”; and (4) “Information Security Awareness” AND “Cybersecurity”. To collect the most recent and contextually relevant empirical data, the review was restricted to publications published between 2020 and 2025. Only English-language conference papers and peer-reviewed journal publications were considered.

INFORMATION GATHERING PHASE

During the information gathering phase, the research study-related papers were downloaded from these five main online academic databases from the source selection phase. Articles identified through the database searches were subject to a three-stage screening process. In the first stage, after examining the articles, all redundant and duplicate articles were removed based on the relevancy of their title and keywords. In order to verify their direct connection to the study’s goal, the papers were re-screened in the second stage using their abstracts and conclusions. The third stage consisted of a full-text evaluation of the remaining papers with a more concentrated screening. The articles were selected here based on inclusion and exclusion criteria, which include addressing security behaviour models or theory, investigating elements that influence or change an individual’s security behaviour, and being empirical or proposing a theoretical framework that has been verified in a cybersecurity setting. Articles that did not discuss a security behaviour model or behavioural factors influencing security practices were excluded. Over a 5-year period spanning from 2020 to 2025, a total of 173 articles were retrieved.

ANALYSIS PHASE

In the analysis phase, five core security behaviour models were extracted from the screened articles. The articles include Protection Motivation Theory, Theory of Planned Behaviour, Theory of Reasoned Action, Fogg Behaviour Model, and Knowledge-Attitude-Behaviour Model. Information relevant to the research focus area was extracted from these articles using a pre-determined set of inclusion criteria and a synthesis matrix table was constructed. It was also observed that in some of the earlier research a mixed strategy was followed, in which several security behaviour models were combined in one analysis. In the concluding phase, all the collected information was reviewed in detail and the conclusions obtained from the review were compiled and presented in the results and findings section.

HUMAN SECURITY BEHAVIOUR MODELS

The SLR identified main information security behaviour models which are Protection Motivation Theory (PMT), Theory of Reasoned Action (TRA), Theory of Planned Behaviour (TPB), Knowledge-Attitude-Behaviour Model (KAB), and Fogg Behaviour Model (FBM). Some of the previous studies have used hybrid or integrated models, which are a combination of two or more of these models to provide a more complete picture of security behaviour

components. Moreover, in these previous studies have also shown that the quantitative method is the most widely used in investigation technique for analyzing the human security behaviour. Questionnaires and surveys are commonly used instruments for collecting data to be investigated and analysed. An overview of comparison of these models including their theoretical foundations, key elements, and primary purposes in cybersecurity scenarios is provided in Table 1.

TABLE 1. Comparative Overview of Human Security Behaviour Models

Models	Theoretical Origin	Core Elements	Description
Protection Motivation Theory (PMT)	Rogers (1975); then revised again by Maddux & Rogers (1983).	Perceived Vulnerability, Perceived Severity, Maladaptive Rewards, Response Efficacy, Self-Efficacy, Response Costs.	Explains how people are motivated to engage protective security behaviours by threat and coping assessments.
Theory of Reasoned Action (TRA)	Fishbein & Ajzen (1975)	Attitude toward behaviour, Subjective Norm, Behavioural Intention.	Predicts voluntary behaviour through attitudinal and normative influences on behavioural intention.
Theory of Planned Behaviour (TPB)	Ajzen (1985; 1991)	Attitude toward behaviour, Subjective Norm, Perceived Behavioural Control, Behavioural Intention.	Expands TRA to include perceived control over behaviour as a further predictor of intention and action.
Knowledge-Attitude-Behaviour (KAB)	Rooted in Bloom (1956); applied by Kruger & Kearney (2006)	Knowledge, Attitude, Behaviour.	Provides a sequential framework linking security knowledge to attitudinal change and protective behaviour.
Fogg Behaviour Model (FBM)	Fogg (2009)	Motivation, Ability, Trigger/Prompt.	Identifies the conditions under which target behaviours occur by examining motivation, ability, and prompts.

PROTECTION MOTIVATION THEORY (PMT)

Protection Motivation Theory (PMT) is a behavioural framework which frequently adopted by researchers in the field of information security (Ogbanufe & Ge, 2023; De Kimpe et al., 2022). The theory was originally introduced by R.W. Rogers (Rogers, 1975) and subsequently refined by Maddux and Rogers (1983). In its early form, PMT in its first version was designed to address disease prevention and health promotion behaviours. Over time, however, its application has expanded considerably, and it is now widely used to examine how individuals behave in relation to information security (De Kimpe et al., 2022). Although initially developed to explain health-protective behaviour in response to fear appeals, PMT has been extensively applied to explain and predict individuals' intentions to engage in cybersecurity practices. The Protection Motivation Theory Model framework is in Figure 2.

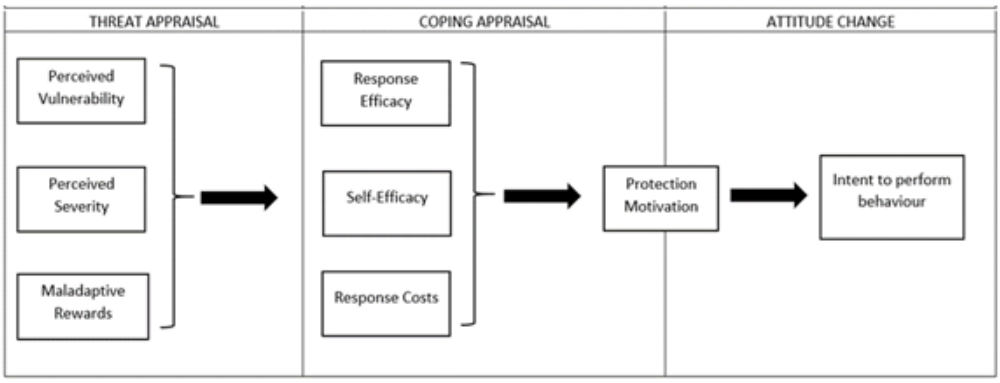

FIGURE 2. Protection Motivation Theory Model (PMT)

The original edition of PMT is the one that focused on fear appeals (Bigsby & Albarracín (2022). It contains two main cognitive appraisal processes. Threat appraisal which includes Perceived Vulnerability and Perceived Severity, and Coping appraisal, represented by Response Efficacy (Marikyan & Papagiannidis, 2023). Threat Appraisal evaluates the danger posed by a threat, encompassing Perceived Severity (the magnitude of potential harm) and Perceived Vulnerability (the individual's subjective probability of experiencing that harm). Coping Appraisal measures how well an individual can respond effectively, including Response Efficacy (perceived effectiveness of the recommended protective action), Self-Efficacy (confidence in one's ability to perform the action), and Response Costs (perceived effort, time, or financial cost of adoption). The revised model also incorporates Maladaptive Rewards, which represent the perceived benefits of continuing risky behaviours (Bigsby & Albarracín, 2022). The components in Protection Motivation Theory is in Table 2.

TABLE 2. PMT Components – Threat Appraisal (Marikyan & Papagiannidis, 2023)

Threat Appraisal-Components	Description	Cybersecurity Example
Perceived Severity	The level of damage or unfavourable implications that might occur if the threat event were to happen.	Financial loss, identity theft, or data breach resulting from a cyberattack.
Perceived Vulnerability	The individual's subjective assessment of the possibility that the threat will directly affect them.	Belief that one's own device is at risk of malware infection.
Maladaptive Rewards	Benefits seen from maintaining a risky conduct rather than adopting recommended safe practice.	Convenience of reusing a single, easily remembered password across multiple accounts.

TABLE 3. PMT Components – Coping Appraisal (Marikyan & Papagiannidis, 2023)

Coping Appraisal-Components	Description	Cybersecurity Example
Response Efficacy	Belief that the recommended preventive intervention will be effective in preventing the threat or decreasing it to a tolerable level.	"Implementing two-factor authentication serves as an effective measure in substantially lowering the likelihood of unauthorised account access".
Self-Efficacy	Confidence on one's ability to successfully take the necessary precautionary measure.	"I am capable of configuring and consistently using a password manager."
Response Costs	Perceived psychological, temporal, financial, or effort cost of adopting the protective behaviour.	"Setting up a password manager is too time-consuming and inconvenient."

In cybersecurity research, PMT has been employed to study diverse protective behaviours including password management, software update compliance, phishing avoidance, and use of security software (De Kimpe et al., 2022). PMT is a psychological model that is commonly used to describe and predict a person's intention and future actions to protect themselves or their organization against a potential attack. PMT offers a robust framework for designing security communications and training programmes that leverage both fears appeal and empowerment strategies. By addressing both threat perception and coping capacity, PMT-informed interventions can be tailored to specific threat contexts and user populations (Bigsby & Albarracín, 2022). A fundamental shortcoming of the PMT is that it relatively ignores social and environmental elements such as organisational norms or peer influence that may also influence security conduct.

THEORY OF REASONED ACTION (TRA)

One of the first psychological frameworks used to forecast voluntary human behaviour was the Theory of Reasoned Action (TRA), which was created by psychologists Martin Fisbein and Icek Ajzen in their book "Belief, Attitude, Intention, and Behaviour: An Introduction to Theory and Research" (1975).

TRA was designed as a more precise and thorough framework for forecasting and analyzing intentional, voluntary behaviour amongst humans (Sheppard et al., 1988). Behavioural intention is identified as the primary precursor of actual behaviour. The two main elements of TRA are subjective norms (the sense of social pressure from important individuals to execute or refrain from the behaviour) and perspective toward the behaviour (the individual's favorable or unfavorable opinion of carrying out the action) (Sheppard et al., 1988). Attitude and subjective norms were combined to generate intention. This intention then inspires the ultimate behaviour, or behavioural intention (Fishbein & Ajzen, 1975). Theory of Reasoned Action Model framework shown in Figure 3.

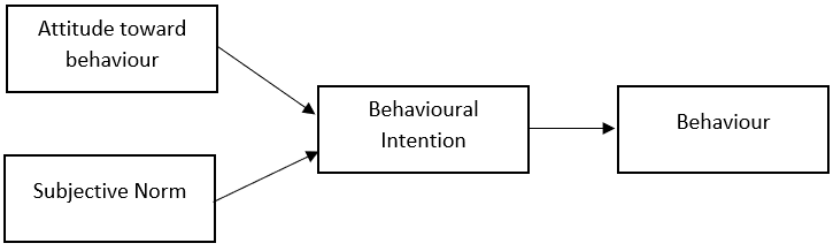

FIGURE 3. Theory of Reasoned Action

Theory of Reasoned Action components is provided in Table 4.

TABLE 4. Theory of Reasoned Action Components (Sheppard et al., 1988)

Component	Description	Cybersecurity Example
Attitude toward the behaviour	An individual's analysis of engaging in a particular behaviour, whether acceptable or unacceptable.	Believing that using a password manager will improve account security (positive attitude).
Subjective Norms	Perceived peer pressure to participate in or abstain from a behaviour.	Feeling pressure from management to apply mandatory Operating System updates promptly.

Component	Description	Cybersecurity Example
Behavioural Intention	The intention of the person to conduct the security behaviour, influenced by attitude and standards.	Intending to update the operating system because it is valued personally and expected organisationally.

In cybersecurity contexts, TRA has been applied to predict security-related intentions such as compliance with security policies, use of security tools, and avoidance of risky online behaviours (Pollini et al., 2022). The model's strength is its capacity to identify social impact and individual evaluative judgements as factors influencing behavioural intention. However, TRA's widely knowledge drawback is its presumption that people have complete voluntary control over their actions.

The model's capacity to accurately anticipate behaviour becomes compromised when external circumstances, such as organisational policies, technical challenges, or lack of skills, restrict actual performance. It was this limitation that led Ajzen to develop the Theory of Planned Behaviour as extension of the original framework.

THEORY OF PLANNED BEHAVIOUR

The Theory of Planned Behaviour (TPB), initially introduced by Ajzen (1985) and later refined in 1991, extends the Theory of Reasoned Action (TRA) by addressing its primary limitation through the addition of Perceived Behavioural Control (PBC) as a third antecedent of behavioural intention. Ajzen (1991) recognised a key limitation of TRA, knowing that it only addressed behaviours entirely within an individual's voluntary control. He responded by expanding the theory in 1985 and developing the Theory of Planned Behaviour (TPB), then was further refined in 1991. TPB expands on TRA by incorporating its two original components, that is attitudes toward the behaviour and subjective norms, alongside the newly added third component, perceived behaviour control. When taken as a whole, these three variables affect how much an individual intends to perform in a specific behaviour (Zwilling et al., 2022). Ajzen acknowledged that not all behaviours are fully controlled by will; people's intentions and actual behaviour are influenced by how easy or difficult they perceive a behaviour to be. Theory of Planned Behaviour Model framework is in Figure 4.

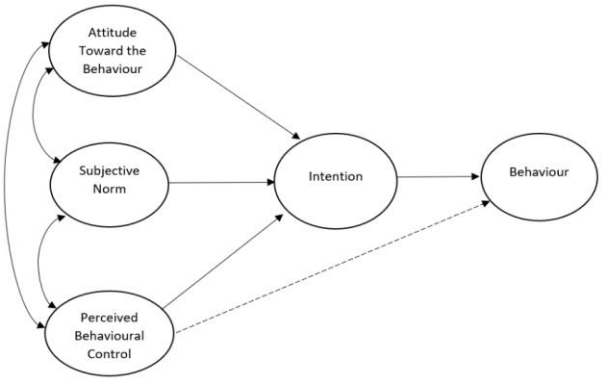

FIGURE 4. Theory of Planned Behaviour (Ajzen, 1991)

TPB has widely used in cybersecurity research to predict phishing reporting behaviour, software update initiation, password management procedures, and security compliance. The model proves especially useful given that PBC directly accounts for factors such as resource

availability, technical proficiency, and system usability, all of which influence the extent to which individuals are able to translate their security intentions into action (Ajzen, 1991). Theory of Planned Behaviour components are provided in Table 5.

TABLE 5. Theory of Planned Behaviour Components (Ajzen, 1991)

Component	Description	Cybersecurity Example
Attitude toward the behaviour	An individual's positive or negative attitude towards the performance of a specific security behaviour, which affects their behavioural intention to perform the behaviour.	An employee believes reporting phishing emails protects the organisation, but he also finds it inconvenient and wasting time to report it.
Subjective Norms	Social pressure to perform or not perform a particular behaviour from management or peers.	Organisational policy requiring the immediate reporting of all suspicious emails creates felt compliance pressure.
Perceived Behavioural Control	The degree to which an individual perceives a behaviour as manageable or challenging, based on the resources and capabilities at their disposal.	Availability of a one-click 'Report Phishing' toolbar button reduces perceived difficulty of reporting.
Behavioural Intention	Readiness to perform the behaviour, shaped by the above three antecedents.	Employees forms the intention to report the suspicious email immediately upon receipt.

TPB's inclusion of PBC has significant implications for cybersecurity system design. Empirical evidence generally supports the predictive superiority of TPB over TRA in non-volitional cybersecurity contexts, where users face barriers such as technical complexity or competing work demands. Notwithstanding its strengths, TPB has been criticised for its static representation of behaviour, its limited treatment of habit and automaticity, and its reduced predictive validity when intention-behaviour gaps are large.

KNOWLEDGE-ATTITUDE BEHAVIOUR (KAB) MODEL

The Knowledge-Attitude-Behaviour (KAB) model is a well-known model in the behavioural psychology and public health education of the 20th century. Its application to information security draws on Bloom's taxonomy of educational objectives (1956) and Webb's Depth of Knowledge model, which together provide a hierarchical conceptualisation of learning and behavioural outcomes (Harris & Patten, 2015). Its application to information security has been attributed to foundational work by Siponen (2000) and Kruger and Kearney (2006), who adapted the model to measure and improve security awareness and behaviour in organisational settings (Kovacevic et al., 2020). Knowledge-Attitude-Behaviour Model is shown in Figure 5.

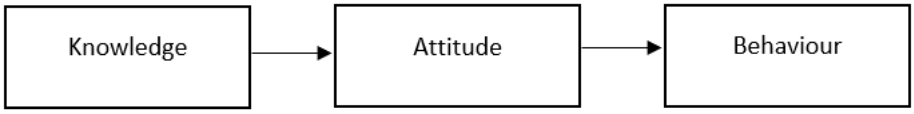

FIGURE 5. Knowledge Attitude Behaviour Model (Siponen, 2000) (Kruger & Kearney, 2006) (Harris & Patten, 2015)

The KAB Model operationalises a step-by-step process: protective behaviour is motivated by positive attitudes, which are informed by security knowledge. The model is especially well-suited for the development and assessment of security awareness and training programs

because of its linear progression (Zwilling et al., 2022). The components in KAB model is shown in Table 6.

TABLE 6. KAB Model Components (Sas et al., 2021; Alkhazi et al., 2022; Pollini et al., 2022)

Components	Description	Cybersecurity Example
Knowledge	Understanding of security threats, risks, vulnerabilities, and appropriate protective actions.	When an employee gets notification that there is an update, they know that software updates need to be implemented. They also able to detect phishing email.
Attitude	How strongly an individual value and recognises the importance of a security measure, which in turn encourages a positive attitude toward taking protective action.	The employee believes two-factor authentication as a crucial security measure and knows that ignoring update alerts presents a genuine security risk.
Behaviour	The actual security behaviour of an individual is a consequence of his/her awareness and positive attitude towards protection.	The employee instantly applies the security patch employs a different password for each account, and reports any odd-looking email to the IT department for further analysis.

The KAB model is often used to measure the effectiveness of cybersecurity interventions by comparing pre-intervention and post-intervention changes in each construct (Kearney & Kruger, 2006; Pollini et al., 2022). Its fundamental strength is its simple sequential logic, a knowledge-based model in which positive attitudes toward security provide the predisposition toward the adoption of secure behaviours. Basically, the KAB model faces criticism for assuming that individuals behaviour change in a straight line from acquiring knowledge (Knowledge), then their attitude changes (Attitude), and finally their actions change (Behaviour) (Khan et al., 2022). However, previous research studies shows that high levels of knowledge do not always lead to positive attitudes, and favourable attitudes do not always lead to secure behaviour. This is particularly true when there are organizational constraints or conflicting motivations (Alkhazi, 2022).

FOGG BEHAVIOUR MODEL

B.J. Fogg (2009) developed the Fogg Behaviour Model (FBM) based on his research on persuasive technology carried out since the 1990s. By focusing on the conditions needed for a specific behaviour to occur, the FBM provides a unique behavioural perspective in contrast to the intention-focused models discussed above. According to the FBM, three factors which is Motivation (M), Ability (A), and a Prompt or Trigger (P), converge together to produce a target behaviour (B) (Fogg, 2009). This can be defined formally as: B = MAP. The FBM model is shown in Figure 6.

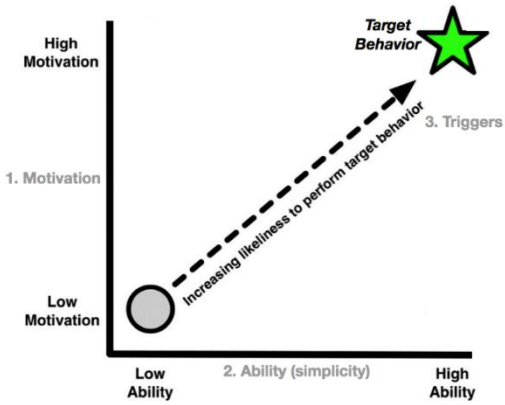

FIGURE 6. Fogg Behaviour Model (Fogg, 2009)

Within this context, persuasion refers specifically to efforts aimed at shaping human behaviour rather than attitudes (Fogg, 2009). Persuasive technology represents an approach that leverages technological means to bring about such behavioural change. To identify the most suitable techniques for guiding individuals toward a desired behaviour, researchers must first understand what drives behavioural change and the mechanisms through which it can be effectively influenced (Mersinas & Bada, 2023). By mapping users' current motivation and ability levels, the model prescribes the type of trigger most likely to elicit the desired behaviour (Fogg, 2009). The components in FBM Model is shown in Table 7.

TABLE 7. Fogg Behaviour Model Components (Fogg, 2009)

Components	Description	Cybersecurity Example
Motivation	The motivation of the person to engage in the desired security behaviour. Hope/fear and pleasure/pain are common examples of motivator	Fear of a malware attack motivates a user to update antivirus settings; hope for improved security motivates adoption of stronger passwords.
Ability	The individual's competence or perceived ease of doing the target behaviour; ability increases when behaviour is simplified.	Automatic file encryption in a designated folder reduces effort to near zero, maximising perceived ability.
Trigger	The signal or indicator that prompts the target behaviour at the right time. Behaviour does not occur without a trigger, even when there is significant motivation and ability.	A pop-up notification stating "Your password is weak, click here to update it now" prompts immediate action.

The FBM specifies four behavioural scenarios based on the intersection of motivation and ability levels: High Motivation/High Ability (HMHA), High Motivation/Low Ability (HMLA), Low Motivation/High Ability (LMHA), and Low Motivation/Low Ability (LMLA) (Shah & Agarwal, 2020). In HMHA, a Signal (an easy reminder) is adequate when both are high, in HMLA a Facilitator (an action-simplifying prompt) is necessary when motivation is high but ability is low, in LMHA a Spark (a motivational prompt) is necessary when ability is high but motivation is low, and lastly in LMLA the target behaviour will not occur regardless of the trigger used when both motivation and ability are low (Wang et al., 2024). With the help of this complex typology, practitioners may design security interventions that are suited for the specific situation.

In cybersecurity, FBM has informed the design of persuasive security interfaces, nudge-based interventions, and adaptive security training systems. Its design-centric orientation

complements the explanatory models (TRA, TPB, PMT, KAB) by translating theoretical insights into actionable system design principles. A notable limitation of FBM is the relative scarcity of large-scale empirical validation studies in information security contexts, and the challenge of operationalising "motivation" and "ability" as measurable constructs in survey-based research.

COMPARATIVE ANALYSIS AND EMERGING TRENDS

A structured comparison of the five models across dimensions relevant to cybersecurity research design, providing a decision aid for model selection are presented in Table 8.

TABLE 8. Comparative Strengths and Limitations of Human Security Behaviour Models

Model	Key Strength	Key Limitation	Best Suited For
PMT	Explicitly incorporates fear appeals; dual appraisal process is well-validated.	Underrepresents social and organisational contextual factors.	Studies on threat communication and security warning design.
TRA	Simple; well-validated for voluntary, deliberate behaviour.	Assumes full volitional control; unsuitable for constrained contexts.	Studies of attitude-driven, voluntary security behaviour
TPB	Extends TRA with perceived behavioural control; strongest predictive validity.	Static model; limited treatment of habit and automaticity.	Organisational security policy compliance and phishing studies.
KAB	Directly applicable to training design and evaluation; intuitive structure.	Assumes linear K→A→B causal chain; empirically contested.	Security awareness training programme design and evaluation.
FBM	Design-centric; actionable for technology-based interventions.	Limited large-scale empirical validation in cybersecurity.	Persuasive security system design and nudge-based interventions.

The increasing use of hybrid or integrated model approaches, in which researchers merge components from two or more framework to solve the shortcomings of any one model, is a prominent trend in the reviewed literature. For instance, a number of researches combine KAB and FBM to bridge the gap between awareness measurement and behavioural intervention design, or integrate TPB with PMT to concurrently account for threat appraisal and perceived behavioural control. These integrative methods are indicative of the rising acknowledgement that security behaviour is a complex and varied phenomenon that cannot be effectively addressed by one theoretical framework.

FINDINGS AND DISCUSSION

The systematic review of 173 publications revealed that quantitative research designs particularly survey-based studies utilising validated questionnaire instruments are the predominant methodology employed in information security behaviour research.

Among the five main models, the Theory of Planned Behaviour (TPB) and Protecction Motivation Theory (PMT) were as the most commonly used in human security behaviour research, highlighting their well-established theoretical foundations and extensive empirical support. In furtherance of addressing the ever-changing dynamics of cybersecurity threats, both models have been changed and extended with extra constructs such as organisational commitment, trust, and habit. Despite the fact that Theory of Reasoned Action (TRA) was not

regularly being used in recent literature but this theory is relevant in this study for the context to explore the basic relationships between attitudes, intentions, and behaviours.

In summary, the Fogg Behaviour Model (FBM) was most prominent in research focused on the studies related to behavioural design and persuasive technology. On the other hand, Knowledge-Attitude-Behaviour (KAB) Model was mainly used in studies assessing the effectiveness of security training programs. As a result, applying hybrid approaches by integrating multiple models would be able to better represent the complex, multidimensional factors impacting security behaviour.

The findings addressed the awareness-behaviour gap observed throughout the literature review. This finding reveals that even when individuals have strong security knowledge and hold positive attitudes towards cybersecurity, nevertheless, this often does not lead to individual consistent protective actions in fact. Factors including situational constraints, habitual behaviours, cognitive biases, and a lack of effective behavioural trigger could drive the discrepancy and present a research gap in this study. The FBM and TPB are found specifically suits the requirements to addressing the research gap as these models explicitly examine other vital elements such as “perceived control”, “ability”, and “situational cues”.

Future research could incorporate the sustainable behaviour outcomes, cross-cultural diversity, digital literaacy, AI-influenced threat perception (eg. AI anxiety, algorithmic aversion, and AI risk perception) and telecommuting settings.

CONTRIBUTIONS TO RESEARCH

This research study contributes four key insights to the literature on human security behaviour models and theories:

First of all, 173 publications from journals and conference papers have been retrieved to identify and assess important elements of human security behaviour models and theories usedin the field of cybersecurity research. From the data synthesis and analysis, five commonly used theories and models in cybersecurity research include Protection Motivation Theory (PMT), Theory of Reasoned Action (TRA), Theory of Planned Behaviour (TPB), Knowledge-Attitude-Behaviour (KAB) Model, and the Fogg Behaviour Model. This summarizes from 54 different theories and models found in previous studies. The findings from data synthesis and analysis will help researchers in cybersecurity field a clearer theoretical roadmap to study human security behaviour.

Secondly, the comparative analysis proves that cognitive, affective, and social variables (eg. attitudes, subjective norms, perceived control) are positively associated with the occurrence of safe cyber behaviour while negative correlations are mostly existent with riskier cyber behaviour along with other factors (eg. motivation, aptitude, and triggers). These findings further help cybersecurity researchers to further their understanding of the theory while provide a basis for implementing specific solutions intended to promote behaviour change in cybersecurity contexts.

Third, this study strengthens the narrative about the creation of a “human firewall” by moving focus away from tech-center defenses to people-based approaches. This indicates that much greater measures at the behavioural level are required for gaining secure cyber behaviour in the long run, rather than using technology-driven solutions or awareness-tailored campaigns.

Fourth, this is a systematic four-phase SLR technique maintaining methodological clarity and replicability through defined constructs-clear inclusion criteria. As a methodological point, the synthesis framework constructed in this process can be used as the perspective for future systematic reviews investigating behavioural theories within relevant information security research fields.

CONCLUSION

This study offers a broad synthesis of research published between 2020 and 2025, through a comprehensive and organised analysis of the key theoretical models and frameworks relevant to human security behaviour in cybersecurity. The literature has employed a total of 54 different behaviour theories and models. However, the analysis and synthesis of data from 173 papers found that five security behaviour models, Protection Motivation Theory (PMT), Theory of Reasoned Action (TRA), Knowledge-Attitude-Behaviour (KAB) Model, and Fogg Behaviour Model (FBM), are the most often and widely used in the cybersecurity behaviour study.

The results show the ultimate importance of human factors in determining cybersecurity outcomes. Human error, poor security practice, and vulnerability to social engineering remain the main reasons why businesses get past their technical defenses. This clearly indicates that we must move away from purely technology-centric views to approaches that holistically focus on the technical behaviour and psychology aspects of security systems and solutions.

The theories reviewed especially the TRA, TPB, and PMT, provide effective models to understand the influence of a combination of cognitive processes, social influences, and motivational factors on individual's security behaviour and intentions. The FBM offers a complementary, design-oriented lens that bridges theoretical insights with practical system-level interventions. Meanwhile, the KAB model remains crucial benchmark for the development and assessment of security training programs.

This review leads to several practical recommendations including: (1) cybersecurity training programmes should be grounded in empirically validated behavioural models and not just rely on intuitive, awareness-based approaches; (2) organisational security culture and subjective norms should be explicit targets with behavioural interventions; (3) system designers should use FBM principles to reduce behavioural friction and deliver timely, context-sensitive prompts; and (4) future research should use integrated model approaches to overcome the limitations of individual frameworks.

Suggestions for future research, clear opportunities exist to create and empirically test hybrid behavioural models which integrate concepts from the five frameworks identified in this study. Cross-cultural comparative study, including studies conducted in developing digital economies like Malaysia, will enhance knowledge of how environmental and cultural factors affect behavioural determinants. Longitudinal studies are necessary to investigate how human security behaviour changes over time. The results of the analysis from this study will directly feed the development of a conceptual model that can guide future empirical studies on shaping SME's security behaviour in Malaysia.

ACKNOWLEDGEMENT

This work was supported by the UTAR Research Fund, IPSR/RMC/UTARRF/2024-C2/N02, 2025

REFERENCES

Alkhazi, Bader, Moneer Alshaikh, Sulaiman Alkhezi, and Hamza Labbaci. 2022. "Assessment of the impact of information security awareness training methods on knowledge, attitude, and behavior." *IEEE Access* 10: 132132-132143.

Alsharida, Rawan A., Bander Ali Saleh Al-rimy, Mostafa Al-Emran, and Anazida Zainal. 2023. "A systematic review of multi perspectives on human cybersecurity behavior." *Technology in society* 73: 102258.

Arend, Isabel, Asaf Shabtai, Tali Idan, Ruty Keinan, and Yoella Bereby-Meyer. 2020. "Passive- and not active-risk tendencies predict cyber security behavior." *Computers & Security* 97: 101964. https://doi.org/10.1016/j.cose.2020.101929.

Chaudhary, Sunil. 2024. "Driving behaviour change with cybersecurity awareness." *Computers & Security* 142: 103858. https://doi.org/10.1016/j.cose.2024.103858.

De Kimpe, Lies, Michel Walrave, Pieter Verdegem, and Koen Ponnet. 2022. "What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context." *Behaviour & Information Technology* 41, no. 8: 1796-1808. https://doi.org/10.1080/0144929X.2021.1905066.

Kovačević, Ana, Nenad Putnik, and Oliver Tošković. 2020. "Factors related to cyber security behavior." *IEEE Access* 8: 125140-125148. https://doi.org/10.1109/ACCESS.2020.3007867.

Lin, Canchu, and Xin Luo. 2021. "Toward a unified view of dynamic information security behaviors: insights from organizational culture and sensemaking." *ACM SIGMIS Database: The DATABASE for Advances in Information Systems* 52, no. 1: 65-90. https://doi.org/10.1145/3447934.3447940.

Mersinas, Konstantinos, and Maria Bada. 2023. "Behavior change approaches for cyber security and the need for ethics." *In The International Conference on Cybersecurity, Situational Awareness and Social Media*, pp. 107-129. Singapore: Springer Nature Singapore.

Meshkat, Leila, Robert L. Miller, Christine Hillsgrove, and James King. 2020. "Behavior modeling for cybersecurity." In *2020 Annual Reliability and Maintainability Symposium (RAMS)*, pp. 1-7. IEEE, https://doi.org/doi:10.1109/RAMS48030.2020.9153685.

Ogbanufe, Obi, and Ling Ge. 2023. "A comparative evaluation of behavioral security motives: Protection, intrinsic, and identity motivations." *Computers & Security* 128: 103136. https://doi.org/10.1016/j.cose.2023.103136.

Pollini, Alessandro, Tiziana C. Callari, Alessandra Tedeschi, Daniele Ruscio, Luca Save, Franco Chiarugi, and Davide Guerri. 2022. "Leveraging human factors in cybersecurity: an integrated methodological approach." *Cognition, Technology & Work* 24, no. 2 : 371-390. https://doi.org/10.1007/s10111-021-00683-y.

Sangwan, Aarti. 2024. "Human factors in cybersecurity awareness." In *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)*, pp. 1-7. IEEE. https://doi.org/10.1109/ISCS61804.2024.10581139.

Sas, Marlies, Genserik Reniers, Koen Ponnet, and Wim Hardyns. 2021. "The impact of training sessions on physical security awareness: Measuring employees' knowledge, attitude and self-reported behaviour." *Safety Science* 144: 105447. https://doi.org/10.1016/j.ssci.2021.105447.

Sheppard, Blair H., Jon Hartwick, and Paul R. Warshaw. 1988. "The theory of reasoned action: A meta-analysis of past research with recommendations for modifications and future

research." *Journal of consumer research* 15, no. 3: 325-343. https://doi.org/10.1086/209170.

Sulaiman, Noor Suhani, Muhammad Ashraf Fauzi, Walton Wider, Jegatheesan Rajadurai, Suhaidah Hussain, and Siti Aminah Harun. 2022. "Cyber–information security compliance and violation behaviour in organisations: A systematic review." *Social Sciences* 11, no. 9: 386. https://doi.org/10.3390/socsci11090386.

Tikanmäki, Ilkka, and Harri Ruoslahti. 2024. "Human Factors Make or Break Cybersecurity!" *Information & Security: An International Journal*. https://doi.org/10.11610/isij.5522.

Triplett, William J. 2022. "Addressing human factors in cybersecurity leadership." *Journal of Cybersecurity and Privacy* 2, no. 3: 573-586. https://doi.org/10.3390/jcp2030029.

Wang, Ying, Linlin Chen, and Wanqing Wang. 2024. "Factors influencing users' willingness to use visual training applications: ARCS motivation theory and Fogg's behavioral model." *International Journal of Industrial Ergonomics* 100: 103556.

Yeoh, William, Marina Liu, Malcolm Shore, and Frank Jiang. 2023. "Zero trust cybersecurity: Critical success factors and A maturity assessment framework." *Computers & Security* 133: 103412. https://doi.org/10.1016/j.cose.2023.103412.

Yeoh, William, Shan Wang, Aleš Popovič, and Noman H. Chowdhury. 2022. "A systematic synthesis of critical success factors for cybersecurity." *Computers & Security* 118: 102724. https://doi.org/10.1016/j.cose.2022.102724.

Zwilling, Moti, Galit Klien, Dušan Lesjak, Łukasz Wiechetek, Fatih Cetin, and Hamdullah Nejat Basim. 2022. "Cyber security awareness, knowledge and behavior: A comparative study." *Journal of Computer Information Systems* 62, no. 1: 82-97. https://doi.org/10.1080/08874417.2020.1712269.

Shah, Pintu R., and Anuja Agarwal. 2020. "Cybersecurity behaviour of smartphone users through the lens of fogg behaviour model." In *2020 3rd International Conference on Communication System, Computing and IT Applications (CSCITA)*, pp. 79-82. IEEE,. https://doi.org/10.1109/CSCITA47329.2020.9137773 .

Ajzen, I., & Fishbein, M. 1988. Theory of reasoned action-Theory of planned behavior. *University of South Florida*, 67-98.

Harris, Mark A. 2015. "Using bloom's and webb's taxonomies to integrate emerging cybersecurity topics into a computic curriculum." *Journal of Information Systems Education* 26, no. 3: 219-234.

Siponen, Mikko T. 2022. "A conceptual foundation for organizational information security awareness." *Information management & computer security* 8, no. 1 (2000): 31-41.

Bigsby, Elisabeth, and Dolores Albarracín. "Self-and response efficacy information in fear appeals: A meta-analysis." *Journal of Communication* 72, no. 2: 241-263.

Siponen, Mikko T., and Jorma Kajava. 1998. "Ontology of organizational IT security awareness-from theoretical foundations to practical framework." In *Proceedings Seventh IEEE International Workshop on Enabling Technologies: Infrastucture for Collaborative Enterprises (WET ICE'98) (Cat. No. 98TB100253)*, pp. 327-331. IEEE,

Fogg, Brian J. 2009. "A behavior model for persuasive design." In *Proceedings of the 4th international Conference on Persuasive Technology*, pp. 1-7.

Fogg, Brian J. "Persuasive computers: perspectives and research directions." In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pp. 225-232. 1998.

Ajzen, Icek. 1991. "The theory of planned behavior." *Organizational behavior and human decision processes* 50, no. 2: 179-211.