Gordon Institute of Business Science
University of Pretoria

Through a prime lens: a review of the extension of Protection Motivation Theory to study user information security behaviours within organisations

24133273

A research project submitted to the Gordon Institute of Business Science, University of Pretoria, in partial fulfilment of the requirements for the degree of Master of Philosophy (Evidence Based Management).

30 June 2025

Abstract

Information security breaches have become more prevalent and severe for organisations, with users often being labelled as both the cause of such breaches and, lately, the first line of defence against such breaches. The dual role of users in information security has led to the study of user information security behaviour, especially in understanding the factors that influence users' motivation to behave in a manner that enhances or exposes organisational information security. Behavioural Information Security, a field dedicated to the study of user information security behaviour, has emerged and grown to provide a sturdy foundation for scholarly advancements in the field; however, the literature has remained contradictory and divergent.

Although reviews have been conducted to address the disjointed literature, this review employs Protection Motivation Theory as a primary theory to synthesise the literature, examining how it has been extended in specific contexts. In doing so, it highlights how the theory is integrated with others to understand user behaviour in organisational information security, using a common base.

This paper reviews existing literature using the PRISMA framework, identifying and analysing prominent academic research papers in Behavioural Information Security. Eight dimensions that share commonalities with the Protection Motivation Theory in Behavioural Information Security were highlighted. These eight dimensions are examined, gaps identified, and a roadmap for future research is provided.

Keywords

Behavioural Information Security; Protection Motivation Theory; Cybersecurity

Declaration

I declare that this research project is my own work. It is submitted in partial fulfilment of the requirements for the degree of Master of Philosophy Evidence Based Management at the Gordon Institute of Business Science, University of Pretoria. It has not been submitted before for any degree or examination in any other University. I further declare that I have obtained the necessary authorisation and consent to carry out this research.

24133273 30 June 2025

Table of Contents

List of Figures

List of Tables

1. Section 1: Introduction

Information security has become a focal area of research due to the increasing likelihood and potential disastrous consequences of cyber breaches for organisations. The World Economic Forum (2025) reported a significant increase in social engineering attacks in 2024, with 42% of organisations experiencing a successful breach. In addition, Zscaler (2024) found a 58.2% increase in global phishing attacks was found in 2023. According to IBM (2024), social engineering and phishing attacks can severely harm organisations, with an average cost of USD 4.88 million per attack. Alarmingly, the use of adversarial generative artificial intelligence is expected to increase the prevalence, evasiveness, and sophistication of these attacks (Schmitt & Flechais, 2024).

Social engineering attacks often use phishing emails to psychologically manipulate users into taking action or revealing information (Goel et al., 2017). Users are seen as both the leading cause of breaches and a strategic asset for improving organisational information security efforts (Crossler et al., 2013). In other words, users have been shown to be the cause and solution to information security challenges.

The dialectical tension of users as contributors to and mitigators of information security breaches has prompted scholars to explore the organisational and individual factors that drive users to protect information assets and what influences their information security behaviour (Dalal et al., 2022; Dodge et al., 2023; Lee et al., 2008). User information security behaviour involves actions taken by users to safeguard organisational information via data backups and antivirus software (Boss et al., 2015), or applying security settings to personal devices when accessing organisational information (Bélanger et al., 2022), reporting and responding to suspicious phishing emails (Bayl-Smith et al., 2022), and complying with organisational information security policies (Safa et al., 2016). No concise definition exists, but user information security behaviour refers to actions or inactions by users to safeguard organisational information.

The behavioural factor in information security has spurred the evolution of the Behavioural Information Security subdomain within information systems security. This subdomain examines the complex interactions between users, technology, and organisations to understand user information security behaviour (Crossler et al., 2013; Jeyaraj & Zadeh, 2020; Liang et al., 2023). A key focus of this subdomain is to identify the motivational factors that lead users to enhance organisational information security (Boss et al., 2015).

Behavioural Information Security combines theories from psychology, criminology, and health psychology (Moody et al., 2018; Posey et al., 2013). Although this integrative approach can expand thinking, offer new insights, and advance theory building, it may have had unintended results on Behavioural Information Security research (Dalal et al., 2022; Mou et al., 2022; Okhuysen & Bonardi, 2011)

Despite the wealth of literature in Behavioural Information Security accrued since Dhillon and Backhouse (2001) suggested that human behaviour has a profound impact on successful information security, research findings remain contradictory and divergent (Gerdin, 2025). Scholarly inquiries suggest that incongruent results stem from scholars' differing theoretical lenses used to explain or predict users' information security behaviour (Boss et al., 2015). Some argue that the theoretical context of these studies significantly affects the comparability and harmonisation of findings (Vrhovec & Mihelič, 2021). Others have critiqued the field's over-reliance on cross-sectional and self-reported data, which cannot capture essential longitudinal behavioural shifts (Cram et al., 2024).

The lack of consensus among scholars has led to insufficient generalisability of theoretical contributions. Further, and perhaps most detrimental, some scholars have critiqued the applicability of the foundational theories underpinning Behavioural Information Security research (Van Slyke & Belanger, 2020).

Although true generalisability may be improbable in Behavioural Information Security, a level of theoretical synthesis is still a goal scholars should strive towards to advance the overall information systems research (Gregor, 2006). As such, scholars have endeavoured to reconcile the disparate findings in literature by reviewing and synthesising the theoretical contributions of empirical research. While these reviews offer valuable insights into generalisable factors influencing user information security behaviours, many fall short in adequately addressing key constructs and contextual nuances, often integrating incompatible theoretical perspectives and lacking the application of a coherent foundational theory.

The increasing cyber threats highlight the importance of finding novel ways for organisations to motivate their users to adopt protective behaviours. It is even more critical for scholars to understand what factors influence these behaviours amidst the growing inconsistent literature. To address this, a different approach is taken to reviewing existing literature:

adopting a foundational theory to create uniformity and structure in reviewing disparate studies with a common theoretical base.

Building on the guidance offered by Mou et al. (2022) and Sommestad et al. (2015b), grounding research on a widely accepted theory such as the Protection Motivation Theory and extending its capabilities in nuanced settings using other focused theories can offer new insights. In doing so, it may provide actionable solutions to practitioners that can positively affect user information security behaviour, thereby improving phishing and social engineering resilience, and provide a roadmap for future research in Behavioural Information Security.

The remainder of this section is structured as follows:

- Next, a review of the extant literature and theoretical underpinnings is provided.
- Thereafter, the formulation of the review questions

1.1 Review of extant literature

The earliest conceptualisation of factors influencing users' information security behaviour in organisations led to a taxonomy of influences on user's security behaviour (Leach, 2003). Stanton et al. (2005) extended on this and distinguished between malicious, neutral, and beneficial intent that could influence actions. While insightful, these studies lacked a foundational theoretical lens (Anderson & Agarwal, 2010). Lebek et al. (2014) found that the earliest publications on professionals and employees started in 2007, mainly in conference outlets. Their review confirms prior reviews in this realm, i.e. Siponen (2000a) and Siponen (2000b), but it fell beyond the scope of their review.

Lebek et al. (2014) was instrumental in understanding how various theories were applied and integrated to reinforce the field's theoretical scaffolding by mapping the lay of the land in the literature and advocating the importance of extending research beyond these theories.

Following on this, Moody et al. (2018) extended their research to create a conceptual framework of integrated theories. The authors developed a unified model integrating 11 key theories to understand causal relationships and synthesise research findings. The resulting unified model for information security compliance (UMISPC) included various theoretical constructs. However, the scholars warned that integrating multiple theories without careful consideration could lead to redundancy and competition, neglecting their complementary

roles. They noted that their data fit process indicated possible missing constructs and relationships affecting model fit. Additionally, the final model lacked key theoretical constructs like social and ethical norms and user attitude, essential in Behavioural Information Security (Cram et al., 2019).

Cram et al. (2019), expounded on Moody et al. (2018), compared 401 theoretical constructs from various studies to explain users' compliance with organisational information security policies and may have overlooked that some constructs are irrelevant in workplace contexts, resulting in inconsistent and contradictory findings. (Mou et al., 2022). Okhuysen and Bonardi (2011) refer to this problem as the conceptual distance between the theory and the phenomenon it is called to explain.

Mou et al. (2022), critiquing the work of Cram et al. (2019), provided a holistic review. They noted the influence of Protection Motivation Theory on Behavioural Information Security research and centralised the theory to examine its effectiveness in explaining information security behaviour across contexts. This study focused on a single theoretical lens and tested its boundaries in multiple settings, supporting the theory in many cases.

Some reviews do not study how theories complement or contradict each other. For example, Balagopal and Mathew (2024) conducted a qualitative review of theories explaining users' compliance with information security policies. The study categorised these into moral disengagement, neutralisation and deterrence, stress, monitoring mechanisms, individual decision making, and organisational factors. The review offers insights into themes influencing user information security behaviour through compliance and non-compliance but fails to explain how these themes interact to affect compliance, such as how stress influences decision making or how monitoring affects stress. This highlights the lack of synthesis between theories, as argued by Moody et al. (2018).

Many scholars have demonstrated that employing an anchoring theory or highlighting a specific theoretical lens aids in synthesising existing literature. A collection of meta-analytic studies attempts to synthesise literature through a singular theoretical lens to examine protective behaviour. Trang and Brendel (2019) conducted a meta-review using deterrence theory to understand the use of deterrents in influencing user compliance behaviour. Mou et al. (2022); Sommestad et al. (2015a) used protective motivation theory as a central theory to comprehend user protective behaviour, which may have provided a more solid foundation for future research to build upon.

The existing literature highlights inconsistencies in meta-analyses and reviews regarding theoretical synthesis. These include neglecting contextual matters, combining incompatible theories, repetitive theory combinations, and the absence of a key anchoring theory. This lack of congruence among systematic literature reviews and meta-analyses creates a significant gap in current knowledge.

Although Okhuysen and Bonardi (2011) offers actionable methods to address inconsistencies, yet many were overlooked in numerous studies. The authors emphasise anchoring the research in robust theory and using supplemental theory to enhance the primary theory where necessary.

The previous section summarised the current scholarly debates regarding inconsistent findings in the literature and potential methods to address them. The following section will highlight the rationale for selecting a primary theory as the central theory and formulate an appropriate review question.

1.2 Review Question formulation

Among the common theories found across the literature reviewed that have studied user information security behaviour, the most popular were the 1) Protection Motivation Theory, 2) Deterrence Theory, 3) Social Cognitive Theory, 4) Theory of Planned Behaviour and 5) Neutralisation Theory, among others (Balagopal & Mathew, 2024). Among the theories listed, the Protection Motivation Theory has been marked as the most prevalent theory in Behavioural Information Security because it highlights the psychological processes undertaken by users that influence their protective behaviour (Alrawhani et al., 2025).

Kiran et al. (2024) suggested that Protection Motivation Theory effectively explains and predicts users' information security behaviour. Therefore, it may be considered a Type IV theory in information systems for its explanatory and predictive capabilities behaviour (Gregor, 2006). Type IV theories demonstrate the ability to comprehend the driving factors of the underlying causes and prediction, have clearly defined constructs, and understand the interactions between those constructs well.

As a Type IV Theory, Protection Motivation Theory is a solid foundation for a systematic literature review, providing a rigorously tested lens for studying protection behaviour.

Understanding information security behaviour through this theory reveals gaps, suggesting that combining it with another theory may enhance explanatory ability.

Although reviews and research are abundant in this field, a gap remains in the existing literature, which can be addressed by asking, *"How has the Protection Motivation Theory been extended to study user information security behaviour within organisations?*".

Answering this question will consolidate disparate findings in literature through a unified base using Protection Motivation Theory, highlighting areas where the theory has been extended, and identifying gaps that may require further scholarly attention. In doing so, it provides a roadmap of existing scholarly debates to guide future research.

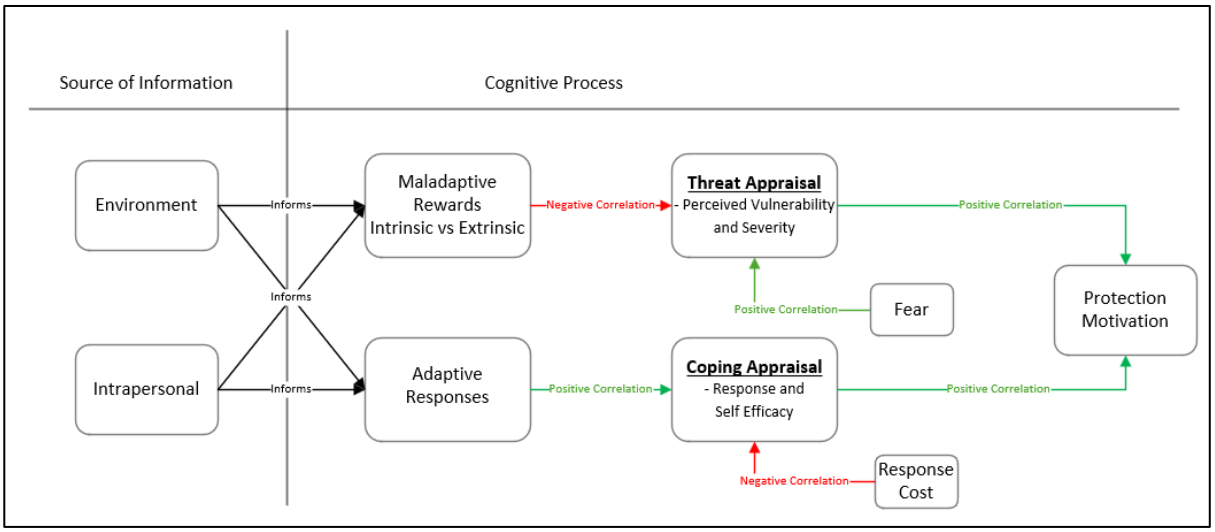
1.3 Anchor Theory - The Protection Motivation Theory

The motivation behind users' behaviour is the core basis of the Protection Motivation Theory (Hanus & Wu, 2015). Protection motivation is a dependent variable influenced by two primary constructs: Threat and Coping Appraisal (Rogers, 1975).

The Protection Motivation Theory was initially developed in the health domain to understand the antecedents that motivate people to respond in a manner that may protect themselves when confronted with a health threat (Rogers, 1975; Rogers, 1983). The original theory suggests that users' motivation to protect against threats is shaped by their appraisal of impact severity, occurrence probability, and belief in their efficacy and helpfulness of the recommended response (Rogers, 1975).

The theory was extended to include sources of information for users' cognitive appraisal. It also accounted for users' consideration of maladaptive and adaptive rewards and fear as a mediating factor enhancing protective motivation (Rogers, 1983). Although the mediating role of fear allows users to cognitively assess the consequences of behaving adaptively or maladaptively, it does not directly influence coping appraisal and protection motivation (Rogers, 1983).

Figure 1- Protection Motivation Theory



Adapted from (Rogers, 1983)

Rogers (1983) suggest that the Protection Motivation Theory is comprised of the following constructs:

- **Threat Appraisal** is the cognitive ability to evaluate the exposure and severity of a threat. It consists of *Perceived Vulnerability,* where the user determines the level of exposure to the threat, and *Perceived Severity,* where the user determines the magnitude of damage the threat can do if realised.
- **Coping Appraisal** – The cognitive ability of the user to understand the requirements to mitigate the threat. Coping appraisal consists of *Response Efficacy* – The certainty that the prescribed method will eliminate the threat. *Self-Efficacy* – The belief that one has the requisite skills to mitigate or eliminate the threat. *Response Cost* – evaluating the feasibility and burden of potential responses against the perceived threat, vulnerability, and severity, determining whether coping efforts are justified.
- **Sources of Information—***Environment:* Factors such as verbal persuasion and observable cues inform the cognitive process. *Intrapersonal*: Factors

such as personality and prior experiences can affect the cognitive process. Any external or intrapersonal source of information can be considered; however, the theory is more concerned with the cognitive mediation process, irrespective of the source of information (Rogers, 1983).

- **Protection Motivation-** A motive aroused by the Coping and Threat Appraisal that directs the subject to act against a harmful and likely threatening event (Rogers, 1983).
- **Fear –** An appeal to incite an emotional response to influence protection motivation (Rogers, 1983).
- **Maladaptive and adaptive responses** – Responses to the threat can be either positive or negative, and can influence the coping and threat appraisal process (Rogers, 1983).

Protection Motivation Theory posits that users engage in protective behaviours when they perceive a severe threat, see themselves as vulnerable, believe in their ability to respond effectively, find maladaptive rewards less appealing than mitigating threats, and view adaptive rewards as more beneficial than the costs (Menard, Bott, et al., 2018; Rogers, 1975; Rogers, 1983).

The human focus of the theory has allowed it to be applied to a wide variety of areas, such as studying tenants' motivation to protect rental homes in the event of a flood, i.e. Oakley et al. (2020); understanding dietary behavioural management in patients with chronic kidney failure, Li et al. (2025); and understanding the behavioural factors driving mobile money protection Seini et al. (2025).

Boss et al. (2015) has argued that Protection Motivation is inextricably linked with users' information security behaviour, and the application of the theory in the behavioural security field can be traced back to when it was used to understand why users fail to protect information even when they know better, and how users react to computer virus threats (Lee et al., 2008; Workman et al., 2008). The theory grew into various sub-fields in the literature, which include studying the role of threat messaging in phishing attacks, i.e. Jansen and van Schaik (2019), the effect of user compliance/non-compliance to information security policies, i.e. Bulgurcu et al. (2010) and users' susceptibility to information security breaches i.e. Desolda et al. (2021).

The theory effectively accounts for and forecasts users' intentions to protect computer information assets, as its constructs, such as threat and coping appraisal, correlate well with information security concepts (Sommestad et al., 2015b). Additionally, the theory is found to be effective primarily because it relies on subtle, fear-based cue vignettes to encourage protective action, making it more sensitive to users (Boss et al., 2015).

Although a broad body of literature differentiates between users' intentions and actual information security behaviour, this review remains impartial.

1.3.1 Full vs Core Nomology of Protection Motivation Theory

The discourse in the Behavioural Information Security domain has been split between using fear as a mediator to incite a positive behavioural response. Boss et al. (2015) tested the Protection Motivation Theory in an organisational setting and posited that any subsequent research employing the theory should utilise fear as a mediator. They established two frameworks, namely the core and full nomology of the theory, which distinguishes a version that incorporates fear (Full Nomology) from one that does not (Core Nomology).

To date, numerous studies have examined fear and its exclusion; however, a consensus is yet to be reached among scholars. Fear is argued to lack the same psychological weight in organisational settings as in personal or health contexts (Warkentin et al., 2016). As such, using fear to encourage positive information security behaviour may be ineffective. In contrast, some studies indicate that fear appeals can positively influence users' behaviour, but caution is necessary when communicating such appeals (Park et al., 2021).

Impactful reviews in the field, each with its nuanced approaches and findings, echo the differences of opinion regarding the support for or against the use of the Core or the Full Nomology of the Protection Motivation Theory (Cram et al., 2019; Lowry et al., 2023; Mou et al., 2022). Despite these differences, this review makes no distinction between studies that have used either the Core or Full nomologies of the theory.

1.3.2 Limitations of the Protection Motivation Theory

Social engineering and phishing leverage human fallibility and vulnerability. Workman (2007) argues that not all factors resulting in a successful breach using social engineering and phishing tactics are cognitive-based but consist of manipulating unconscious and emotional factors such as impulsivity, agreeableness and fear. As Protection Motivation Theory only accounts for a user's ability to process threat situations cognitively, it does not adequately account for situations where unconscious, heuristic and habitual factors are essential. This is seen in studies where Protection Motivation is supplemented with constructs more specialised in these contexts, i.e. (Vance et al., 2012). Furthermore, the theory does not account for social and personal biases, attitudes and norms (Mou et al., 2022).

The limitations of the Protection Motivation Theory suggest that it may be prudent to integrate it with area-specific theories to supplement and strengthen the factors that influence protection behaviour, as seen in empirical literature, for example Ogbanufe et al. (2023) and Ifinedo (2012).

1.4 Summary of Section 1

The section opened by emphasising the increased risk and impact of information security breaches on organisations and highlighted the role of users, and specifically their behaviour, in safeguarding information. It then introduced the user's information security behaviour as the construct under review and positioned it within the Behavioural Information Security domain of study.

The inconsistencies in the existing literature are reviewed, leading to the formulation of the review question. The anchor theory is justified and summarised.

Section 2 will detail the methodological approach employed to answer the review question.

2. Section 2: Method and Analysis

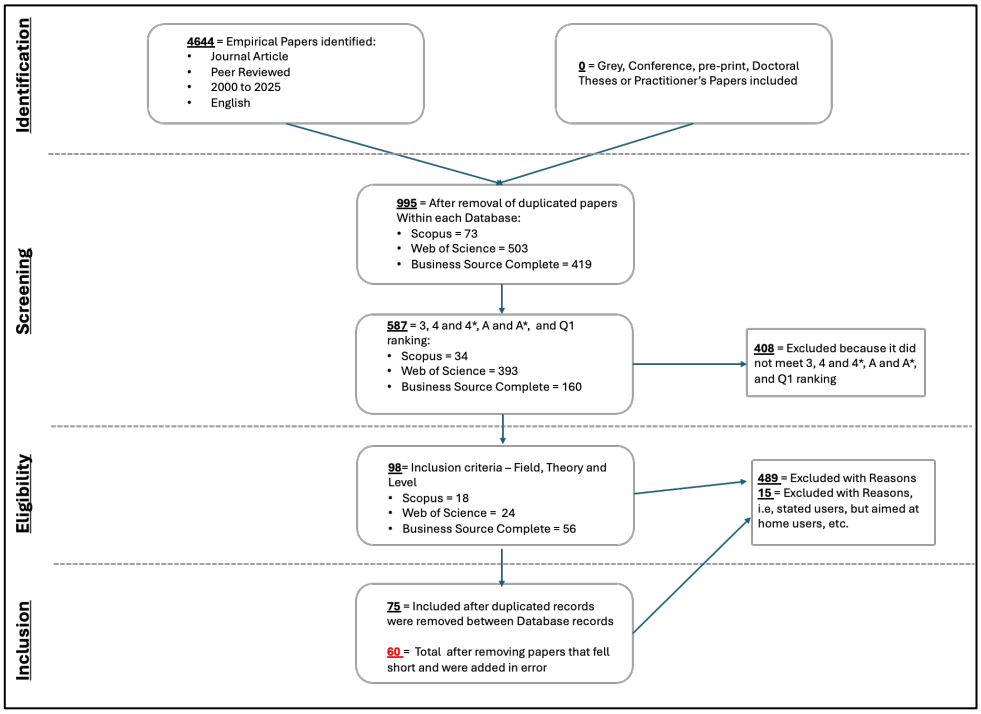
The key characteristics of a high-quality review are its reproducibility, transparency, and rigour, which are demonstrated in the methodology used to validate the study's evidence and findings (Fan et al., 2022). This section is divided into two sections: literature search and literature analysis.

2.1 Literature Search

The first phase employs the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA), a guideline designed to enhance the overall transparency of a Systematic Literature Review (SLR) and ensure a replicable process for searching relevant literature (Page et al., 2021).

Figure 2 illustrates the process used to search for, screen and determine the eligibility for inclusion of each of the identified studies, as defined by PRISMA. The process is divided into four phases: Identification, Screening, Eligibility, and Inclusion. The results are presented following each respective phase.

Figure 2 – Information collection flow according to PRISMA



Source: Adapted from (Liberati et al., 2009)

In reviewing the review question: "*How has the Protection Motivation Theory been extended to study user information security behaviour within organisations?"* the search and evaluation criteria should include 1) the domain of study: e.g. Behavioural Information Security, 2) the theoretical lens: the Protection Motivation Theory, 3) the construct being studied: protective behaviour, and 4) the context: focusing on organisations or employees.

The sources and search strings are developed according to the four criteria outlined. The following section will provide the details and justification of the sources used for the information search.

2.1.1 Identification: Information sources and search strategies

The sources used to search for information must contribute to the field and be rigorously peer-reviewed to ensure quality (Paul et al., 2021). According to Paul et al. (2021), the Web of Science (Wos) and Scopus meet this criterion and, as such, was used as reliable sources of information. These academic search systems were well-suited to provide the literature necessary for evidential synthesis Gusenbauer and Haddaway (2020). EBSCO Business Source Complete (core database) was included to expand the search and minimise potential publication bias by using Scopus and Web of Science exclusively (Mongeon & Paul-Hus, 2015).

In line with the research question, the search keywords and strings were crafted to include the domain of study, the theory to include, the construct under review, and the context in which the study was done. The results are shown in the table below. The search strings were adapted to the search fields on the respective search platforms, as shown in Table 1.

As literature has used various terms interchangeably to describe the domain of study as argued by (Shiau et al., 2023), various terms including "Behavioural Information Security" i.e. Crossler et al. (2013), "Cybersecurity Behaviour" i.e. (Kiran et al., 2024) and (Kim et al., 2024); "Behavioural Information Systems Security" i.e. Liang et al. (2023), "Information Security Behaviour" i.e Chou (2016) and "Information Systems Security Behaviour" i.e Karjalainen et al. (2019) was used. The construct is also recorded by nuanced naming: "Protection Behaviour" (Boss et al., 2015; Lee et al., 2008), "Protective Behaviour" (Dodge et al., 2023). The use of BOOLEAN operators as part of the search string is integral to

systematic searches, and the AND or OR operator is well supported to search for and link single concepts for conceptualisation and synthesis (Gusenbauer & Haddaway, 2020).

Scopus strings and results	**Web of Science Results**	**Business Source Complete Results**
TITLE-ABS-KEY (information AND security) AND TITLE-ABS-KEY (protection AND motivation) OR TITLE-ABS-KEY (pmt) AND TITLE-ABS-KEY (protection AND behaviour) AND TITLE-ABS-KEY (organisation) OR TITLE-ABS-KEY (employee) = **63**	(((TS=(Information Security AND Protection Motivation Theory)) AND PY=(2000-2025))) AND ((LA==("ENGLISH") AND DT==("ARTICLE")) NOT (SILOID==("PPRN"))) **= 487**	(("information security" AND "protective motivation theory" OR "PMT")) = **419**
TITLE-ABS-KEY (information AND systems AND security) AND TITLE-ABS-KEY (protection AND motivation) OR TITLE-ABS-KEY (pmt) AND TITLE-ABS-KEY (protection AND behaviour) AND TITLE-ABS-KEY (organisation) OR TITLE-ABS-KEY (employee) = **27**	(((TS=(Information Systems Security AND Protection Motivation Theory)) AND PY=(2000-2025))) AND ((LA==("ENGLISH") AND DT==("ARTICLE")) NOT (SILOID==("PPRN"))) **= 385**	(("information systems security" AND "protective motivation theory" OR "PMT")) = **419**
TITLE-ABS-KEY (information AND security AND behaviour) AND TITLE-ABS-KEY (protection AND motivation) OR TITLE-ABS-KEY (pmt) AND TITLE-ABS-KEY (protection AND behaviour) AND TITLE-ABS-KEY (organisation) OR TITLE-ABS-KEY (employee) = **63**	(((TS=(Information Security Behaviour AND Protection Motivation Theory)) AND PY=(2000-2025))) AND ((LA==("ENGLISH") AND DT==("ARTICLE")) NOT (SILOID==("PPRN"))**) = 403**	(("information security behaviour" AND "protective motivation theory" OR "PMT")) = **419**
TITLE-ABS-KEY (cybersecurity AND behaviour) AND TITLE-ABS-KEY (protection AND motivation) OR TITLE-ABS-KEY (pmt) AND TITLE-ABS-KEY (protection AND behaviour) AND TITLE-ABS-KEY (organisation) OR TITLE-ABS-KEY (employee) = **20**	(((TS=(Cybersecurity Behaviour AND Protection Motivation Theory)) AND PY=(2000-2025))) AND ((LA==("ENGLISH") AND DT==("ARTICLE")) NOT (SILOID==("PPRN"))) **= 90**	(("cybersecurity behaviour" AND "protective motivation theory" OR "PMT")) = **419**

TITLE-ABS- KEY (behavioural AND cybersecurity) AND TITLE-ABS- KEY (protection AND motivation) OR TITLE -ABS-KEY (pmt) AND TITLE-ABS- KEY (protection AND behaviour) AND TITL E-ABS-KEY (organisation) OR TITLE-ABS-KEY (employee) = **10**	(((TS=(Behavioural Cybersecurity AND Protection Motivation Theory)) AND PY=(2000-2025))) AND ((LA==("ENGLISH") AND DT==("ARTICLE")) NOT (SILOID==("PPRN"))) **= 9**	(("behavioural cybersecurity" AND "protective motivation theory" OR "PMT")) = **419**
TITLE-ABS- KEY (cyber AND security AND behaviour) AND TITLE-ABS- KEY (protection AND motivation) OR TITLE -ABS-KEY (pmt) AND TITLE-ABS- KEY (protection AND behaviour) AND TITL E-ABS-KEY (organisation) OR TITLE-ABS-KEY (employee) = **13**	(((TS=(Cyber Security Behaviour AND Protection Motivation Theory)) AND PY=(2000-2025))) AND ((LA==("ENGLISH") AND DT==("ARTICLE")) NOT (SILOID==("PPRN"))) **= 60**	(("behavioural cybersecurity" AND "protective motivation theory" OR "PMT")) = **419**
TITLE-ABS- KEY (behavioural AND information AND sec urity) AND TITLE-ABS- KEY (protection AND motivation) OR TITLE -ABS-KEY (pmt) AND TITLE-ABS- KEY (protection AND behaviour) AND TITL E-ABS-KEY (organisation) OR TITLE-ABS-KEY (employee) = **28**	(((TS=(Behavioural Information Security AND Protection Motivation Theory)) AND PY=(2000-2025))) AND ((LA==("ENGLISH") AND DT==("ARTICLE")) NOT (SILOID==("PPRN"))) **= 53**	(("Behavioural Information Security" AND "protective motivation theory" OR "PMT")) = **419**
Total Records = 224	Total Records = 1487	Total Records = 2933
After removal of Duplications = 73	After removal of Duplications = 503	After removal of Duplications = 419

Table 1 - Search Strings and Results

2.1.2 Screening

The screening criteria section is a vital part of the review. The criteria were developed to address the research question and are explicitly stated and explained in terms of answering the question, as clarified by Snyder (2019).

Each search string provided in Table 1 considered the following criteria:

- The eligibility period for publication is from 2000 to 2025, as no literature on the socio-organisational view was confirmed before the study by Dhillon and Backhouse (2001). An additional retrospective year was included to cover any potential previous studies that the authors may have missed; consequently, the period from 2000 to 2025 was selected.
- The study must be published in English.
- The study must be published in a 3, 4, or 4* rated journal as outlined by the Academic Journal Guide (AJG) of 2024, or A and A* according to the Australian Business Deans Council (ADBC) journal quality list of 2022, or Q1 in the SCImago Journal and Country Rank (SJR) indicators.
- All conference papers, grey literature, and practitioners' literature were excluded as sufficient peer-reviewed academic literature exists. As argued by Mou et al. (2022), the number of peer-reviewed published papers in this field has increased threefold since 2014, hence there is no need to include these.
- No pre-print studies or doctoral theses are included.

The appropriate filters were enabled on the respective database strings to ensure all returned studies met the abovementioned criteria.

The results of the Scopus, Web of Science, and Business Source Complete searches were downloaded to Microsoft Excel, and a VLookup function was performed against the AGJ, ADBC, and Scimago ranking lists. Of the 73 papers found in Scopus, only 34 conformed to the requisite journal rankings, while of the 419 papers found in Business Source Complete, only 160 met these requirements. The Web of Science returned the highest results in line with the journal ranking requirement, with 393 out of 503 results meeting the requirement.

The screening phase determined that a sample size of 587 papers (34 + 160 + 393) was eligible for analysis.

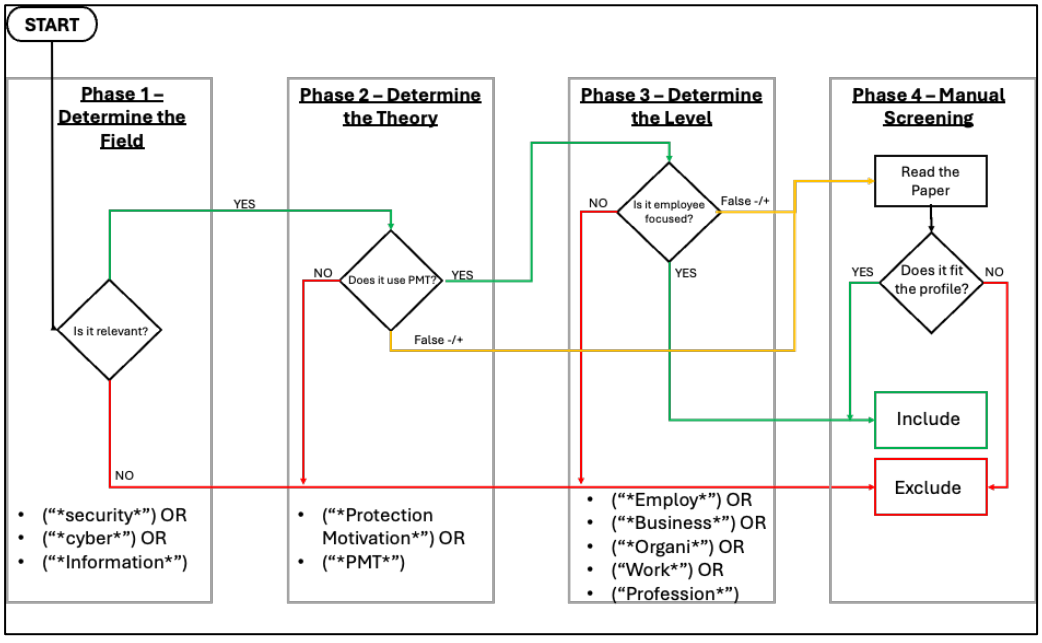
2.1.3 Eligibility

587 papers were included to move to the third eligibility phase. The screening was done against the following criteria:

- The study must be conducted at a micro or meso level. Hemshorn de Sanchez et al. (2021) assert that behaviour is studied at a micro level, while evidence of organisational-level empirical Behavioural Information Security research exists, for example, Vedadi et al. (2024) and Ogbanufe et al. (2023)
- The study must be conducted in the context of information security, information security behaviour, Behavioural Information Security, or behavioural cybersecurity.
- No Information Technology or Computer Science papers are considered.
- The study must have been empirically conducted with employees or organisations.
- The Protection Motivation Theory must be referenced as part of the study, but it should not be the sole theory used.

The reference list of the 587 papers was consolidated in an Excel document and then analysed using Microsoft Excel, in four phases as shown in the graphic.

Figure 3 - Flowchart depicting the screening process



Source: Author's own work

The first phase entails determining if the paper is in the Information Security or Cybersecurity field. This was done using the countif function in Microsoft Excel to perform string recognition against the abstract column of each paper downloaded from Scopus and Business Source Complete. To ensure that the paper was in the field, the countif statement is expounded, for example: countif (Abstract_Column, "*Cyber*") + countif (Abstract_Column, "*security*") + countif (Abstract_Column, "*Information*"). The search strings are also shown in the graphic. If either string is present in the abstract, Microsoft returns "1";"2" or "3" if not, it returns "0". If "0" is returned, it is excluded. Otherwise, it is passed to the next phase.

The second phase involves determining whether the paper employs the Protection Motivation Theory as one of its theoretical frameworks. The countif statement is as follows: countif (Abstract_Column, "*Protection Motivation*") + countif (Abstract_Column, "*PMT*"). If either string is present in the abstract, Microsoft returns "1" or "2"; if not, it returns "0". If "0" is returned, it is excluded. Otherwise, it is forwarded to the next phase. The results were reviewed, and if a false positive or negative is noted (i.e. some papers refer to PMT as Proxy Mean Tests, resulting in a false positive), the paper is sent to phase four for manual intervention, as indicated by the amber line in the graphic.

The third phase determines the level of the research paper. In this phase, the countif statement searches for evidence that the paper focuses on the employee, organisation or business. The countif statement was issued as follows: countif (Abstract_Column, "*Employ*") + countif (Abstract_Column, "*Business*") + countif (Abstract_Column, "*Organi*")+ countif (Abstract_Column, "*Work*")+ countif (Abstract_Column, "*Profess*"). The search strings are also shown in the graphic. If either string is present in the abstract, Microsoft returns "1","2","3","4" or "5"; if not, it returns "0". If "0" is returned, it is excluded. For thoroughness, a review of the results was conducted, and false positive or negative results were passed to phase four for a manual check of the paper's eligibility.

Only 18 of the 34 papers submitted from Scopus for screening were included, and only 24 passed from the 106 papers screened from Business Source Complete. Web of Science yielded the most eligible papers, totalling 56.

98 papers (18 + 24 + 56) met the criteria for inclusion in the review. After duplicates between the three databases were removed, the number of studies included for analysis was 75. The sample was re-read, and it was found that 15 of the 75 studies initially included were not

eligible based on either being conducted with a sample devoid of an organisational context, referenced PMT as something different from Protection Motivation Theory, or being an SLR or Meta-Analysis. This resulted in 60 studies identified for the analysis phase.

2.2 Phase 2: Literature Analysis

This phase will describe how the 60 papers were analysed using the data structure framework proposed by Corley and Gioia (2004) because it provides a method to organise and delineate between first-order concepts as defined by Van Maanen (1979), its second-order themes derived from the relationships between the first-order concepts and the phase will consolidate the second-order themes to provide an overarching dimension(s). Section 3.2 in the following section describes how the overarching dimensions were developed using existing taxonomies and categories from the literature.

2.2.1 First-order concepts: The construct coding process

Adopting a foundational theory for a literature review is suggested to enhance rigour and replicability by providing a structure for analysing the collected literature (Sauer & Seuring, 2023). Furthermore, a theoretical approach enables the review to be effectively coded, as key constructs, relationships, and boundaries of the theory are clearly defined and explained in the existing research (Seuring et al., 2021). The authors advocate for a deductive approach to conducting a structured literature review in settings where literature is studied to explain how a core theory is extended to explain a phenomenon by incorporating insights from external theories.

As a potential Type IV theory (Gregor, 2006), it is argued that the constructs of the Protection Motivation Theory are well defined. As such, the codes are derived from the theory's first-order constructs, which are mapped on a one-to-one basis, for example:

- Perceived Vulnerability = Perceived Vulnerability
- Perceived Severity = Perceived Severity
- Self-Efficacy = Self-Efficacy
- Response-Efficacy = Response-Efficacy, etc.

2.2.2 Second-order Themes: Axial coding process

In this phase, the codes created in the previous phase are grouped into categories and subcategories, and these are compared for similarities and differences to identify any emerging themes, essentially following the Axial coding process (Gioia et al., 2012). The Axial coding process highlights emergent themes, categories, or subcategories by analysing their relationships to the research question (Simmons, 2017).

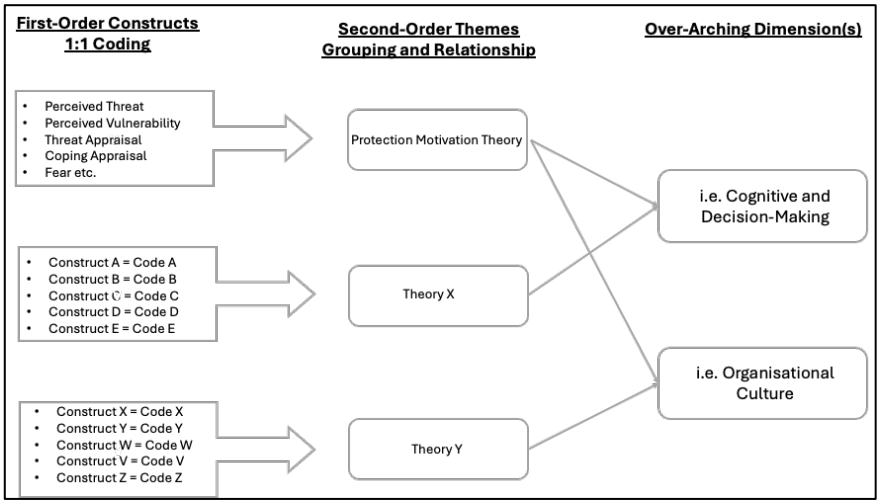
As a potential IV theory (Gregor, 2006), it is argued that the core categories and relationships between the constructs in the Protection Motivation Theory are well understood in the literature. These categories and key relationships are as follows:

- Perceived Vulnerability and Severity are grouped into Awareness of Threat Exposure
- Awareness of threat exposure influences Threat Appraisal.
- Self-efficacy and Response-efficacy = Belief in Threat Response.
- Belief in Threat Response influences Coping Appraisal.

As such, this review adopts a deductive coding process (Fereday & Muir-Cochrane, 2006), where priori codes derived from the theory (Crabtree & Miller, 1992) are applied to the literature being reviewed. In other words, the literature is reviewed using codes derived from the constructs and relationships of the Protection Motivation Theory, which is extended with different theories to explain user protection behaviour in an organisational setting.

A distinction is not made between the core and full nomology of the Protection Motivation Theory to account for all studies that utilise the theory. The figure shows the structure used, whereby first-order constructs are coded, grouped into second-order themes, and subsequently grouped into overarching dimensions, as described by Gioia et al. (2012).

Figure 4 - Example of coding and analysis



Source: Adapted from (Gioia et al., 2012)

Atlas.ti (2025) is used to code the selected papers for the thematic analysis. This will ease the task of tracking and coding various studies across many theories and produce reports for transparency and confirmation of the coding process.

2.3 Assessing any possible bias and limitations

Adherence to the explicit eligibility criteria and search strategies outlined will mitigate the potential selection biases of the review (Snyder, 2019). In addition, publication bias is addressed by including the Business Source Complete to minimise any possible bias observed by only referencing Scopus and Web of Science (Mongeon & Paul-Hus, 2015). Including only literature published in English may slant findings to predominantly English-speaking areas and overlook pertinent findings not specific to English publications.

Following the PRISMA guidelines, the methodology transparently collects, identifies, screens, and analyses the empirical research included in the review, thereby mitigating any possible bias (Beller et al., 2013).

2.4 Summary of Section 2

The section begins by emphasising the importance of detailing the process of identifying and sifting through the studies used in the review, to demonstrate rigour and thoroughness. The section is divided into the search for relevant studies and the analysis of these studies. The first phase highlights the process of selecting academic databases, the search strings used, and how the results were narrowed through journal requirements. It then describes how the studies were refined through the application of eligibility criteria, coded, and analysed.

It closes with a description of the possible biases and limitations. Section 3 will describe the findings from the studies selected in this section.

3. Section 3: Findings from the Literature

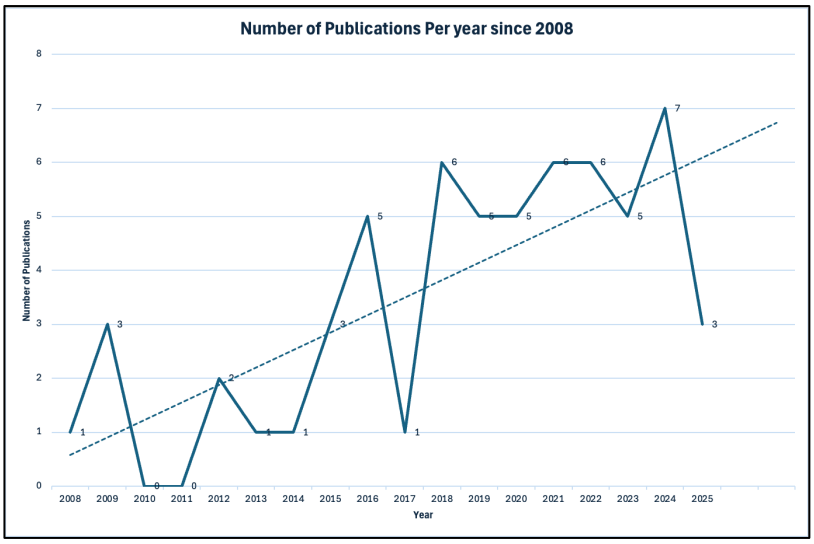
This section will outline the results of the literature search, the analysis of the literature, and the gap between what is known and what is not regarding the review question: "*How has the Protection Motivation Theory been extended to study user protection behaviour within organisations?".* This section comprises two subsections that align the findings with the literature search and analysis outlined in sections 2.1 and 2.2, respectively.

Section 3.1 presents the findings from the literature search, including the number of publications per year, growth trends, prominent journals in the domain, their respective rankings, and the geographic distribution of the literature. Section 3.2 presents the findings of the first- and second-order construct coding, as outlined in Section 2.2. It also details the overall dimensions observed.

3.1 Findings from the Literature Search

The literature in this section comprises 60 empirical papers that meet the eligibility criteria outlined in Section 2.1. Figure 5 shows the frequency of publications per year observed.

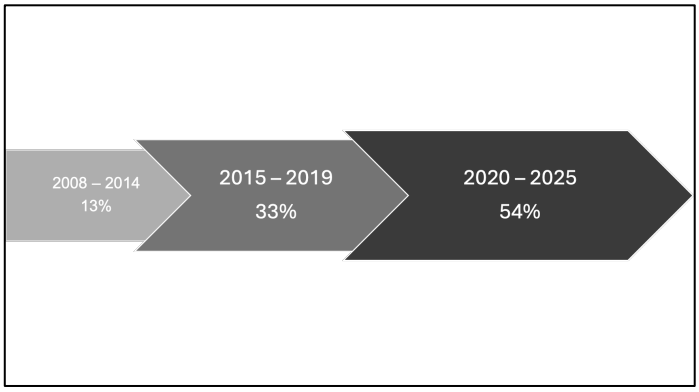
Figure 5 - Frequency of Publications per Year



Source: Author

The growth of publications post-2014 correlates with the findings of Mou et al. (2022), and indicates an interest in the field. Figure 6 illustrates this trend, showing a steep increase in publications post-2014.

Figure 6 - Growth of Publications since 2008



Source: Author

Of the sample collected from 2000, 54% of studies were published between 2020 and 2025, 33% between 2015 and 2019, and the remainder between 2008 and 2014. The period from 2015 to 2025 represents the most activity in the field, accounting for 87%.

Figure 7 - Journals and Ranking of included papers

JOURNAL NAME	SCIMAGO	ABDC 2022	AJG 2024
Australian Journal of Public Administration	Q1	N/A	N/A
Behaviour and Information Technology	Q1	N/A	N/A
Computers and Security	Q1	N/A	N/A
Computers in Human Behavior	Q1	A	2
Computers in Human Behavior Reports	Q1	N/A	N/A
Current Psychology	Q1	N/A	1
Data Base for Advances in Information Systems	Q1	A	2
European Journal of Information Systems	Q1	A*	4
Information and Management	Q1	N/A	3
Information Processing and Management	Q1	N/A	N/A
Information Systems Frontiers	Q1	A	3
Information Systems Journal	Q1	A*	4
Information Systems Research	Q1	A*	4*
Information Technology and People	Q1	N/A	N/A
International Journal of Human-Computer Interaction	Q1	N/A	N/A
International Journal of Information Management	N/A	A*	2
Internet Research	Q1	A	3
Journal of Asia Business Studies	Q1	C	1
Journal of Computer Information Systems	Q1	A	2
Journal of Database Management	Q3	A	1
Journal of Management Information Systems	Q1	A*	4
Journal of Org. Computing & Electronic Commerce	Q2	A	1
Journal of the Association for Information Systems	Q1	A*	4*
MIS Quarterly	Q1	N/A	4*
Pervasive and Mobile Computing	Q1	N/A	N/A

Source: Author

Figure 7 lists the journals and their respective rankings of the included studies. All the journals meet the inclusion criteria outlined in section 2.1.2. A Red, Amber and Green (RAG) method indicates each journal's ranking. If a journal is ranked 3 or 4, rated according to the Academic Journal Guide (AJG) of 2024, or an A according to the Australian Business Deans Council (ADBC) journal quality list of 2022, it is classified as amber. If the journal is rated A*, 4* or Q1 according to the SCImago Journal and Country Rank (SJR) indicators, it is marked as green. The remaining rankings are classified as red or marked as not applicable (n/a) if the journal is not listed.

Figure 8 - Number of publications per Journal per year

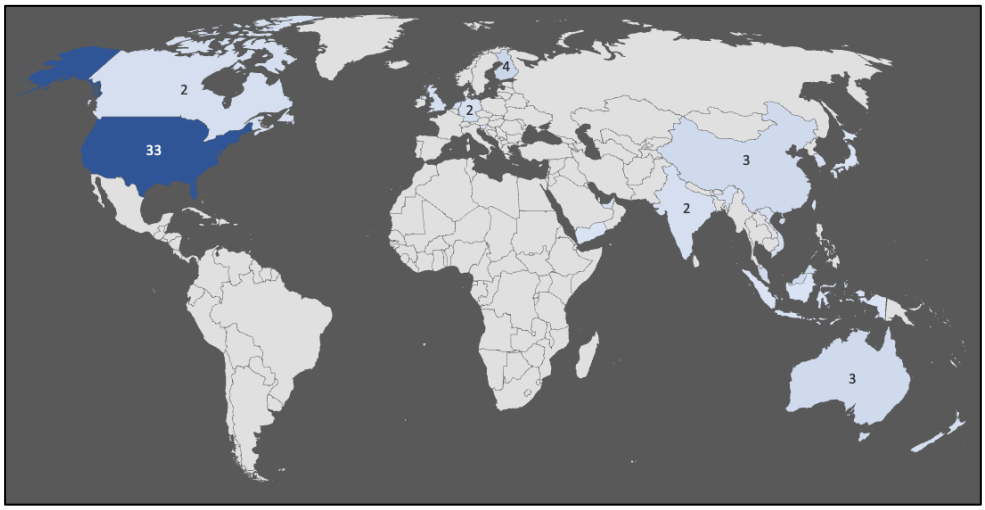
Journal Name/Year	2008	2009	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	Grand Total
Australian Journal of Public Adminisatration														1			1
Behaviour and Information Technology		1					1				1		1			1	5
Computers and Security			1			1			2	2		2	2	4	2		16
Computers in Human Behavior	1						1	1	1		2						6
Computers in Human Behavior Reports													1				1
Current Psychology															1		1
Data Base for Advances in Information Systems									1								1
European Journal of Information Systems		2					1								1		4
Information and Management			1		1												2
Information Processing and Management													1				1
Information Systems Frontiers							1										1
Information Systems Journal												1					1
Information Systems Research												1					1
Information Technology and People				1													1
International Journal of Human-Computer Interaction																1	1
International Journal of Information Management										1			1		1		3
Internet Research																1	1
Journal of Asia Business Studies															2		2
Journal of Computer Information Systems									1			1					2
Journal of Database Management											1						1
Journal of Management Information Systems						1					1						2
Journal of Organizational Computing and Electronic Commerce										1							1
Journal of the Association for Information Systems										1		1					2
MIS Quarterly						1			1								2
Pervasive and Mobile Computing							1										1
Grand Total	**1**	**3**	**2**	**1**	**1**	**3**	**5**	**1**	**6**	**5**	**5**	**6**	**6**	**5**	**7**	**3**	**60**

Source: Author

Figure 8 shows the number of publications per journal per year. Computers and Security, Computers in Human Behaviour, Behaviour and Information Technology, European Journal of Information Systems, and International Journal of Information Management have been the leading outlets for research in Behavioural Information Security over the past 17 years (2008-2025).

Figure 9 shows the geographic focus of the research highlighted in the review.

Figure 9 - Geographical Spread of Research



Source: Author

Table 2 – Geographic locations of study samples

Country	%	Country	%
USA	45%	India	3%
Finland	5%	Netherlands	3%
Australia	4%	New Zealand	3%
China	4%	South Korea	3%
Malaysia	4%	UAE	3%
Canada	3%	UK	3%
EU	3%	Vietnam	3%
Germany	3%	Indonesia	1%
Japan	1%	Taiwan	1%
Slovenia	1%	Yemen	1%

Source: Author

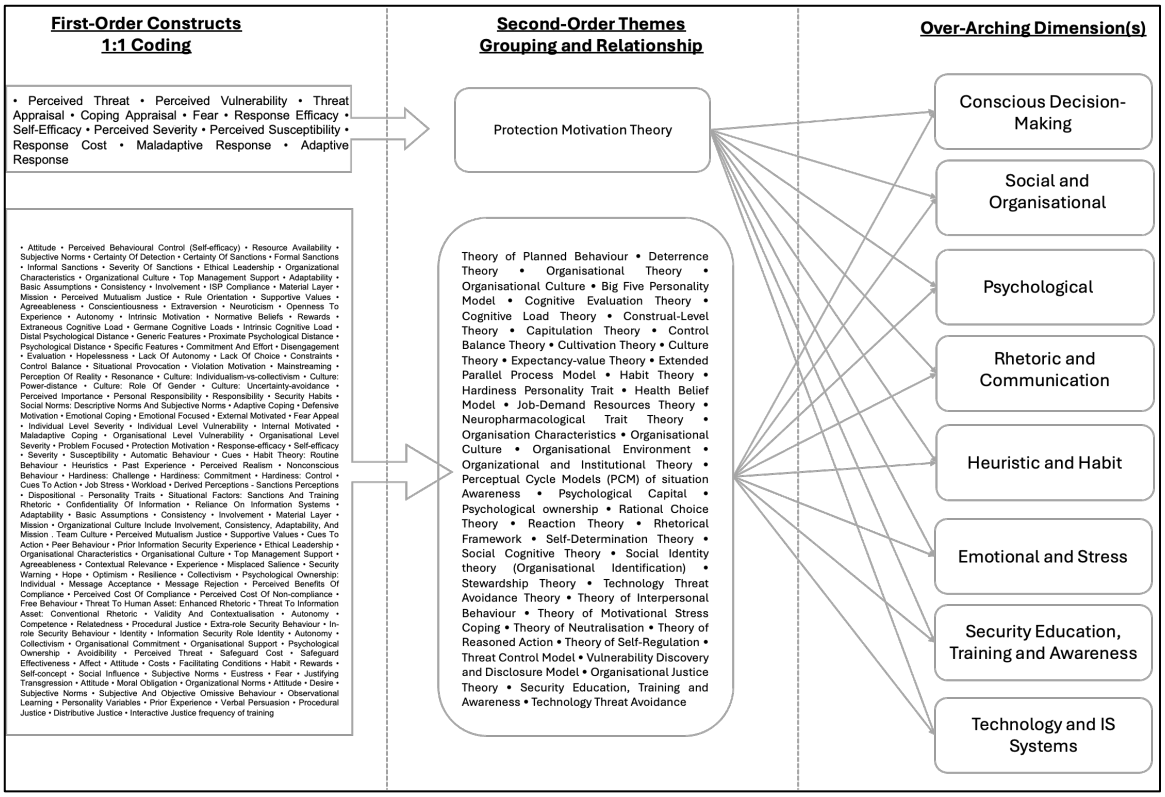
The studies included in this review focused on 20 geographic areas, with the USA accounting for nearly half of the research. The table shows the location of the focus sample, not the location of the journal where the study was published.

3.2 Literature Analysis and Coding

In line with Section 2.2, each of the 60 papers was coded to highlight the first and second-order constructs observed. As discussed, lower-order constructs were coded into higher-order codes to group the various constructs that make up the theories used to study users' behaviour.

First and second-order constructs were coded as shown in Figure 10.

Figure 10 - Coding results

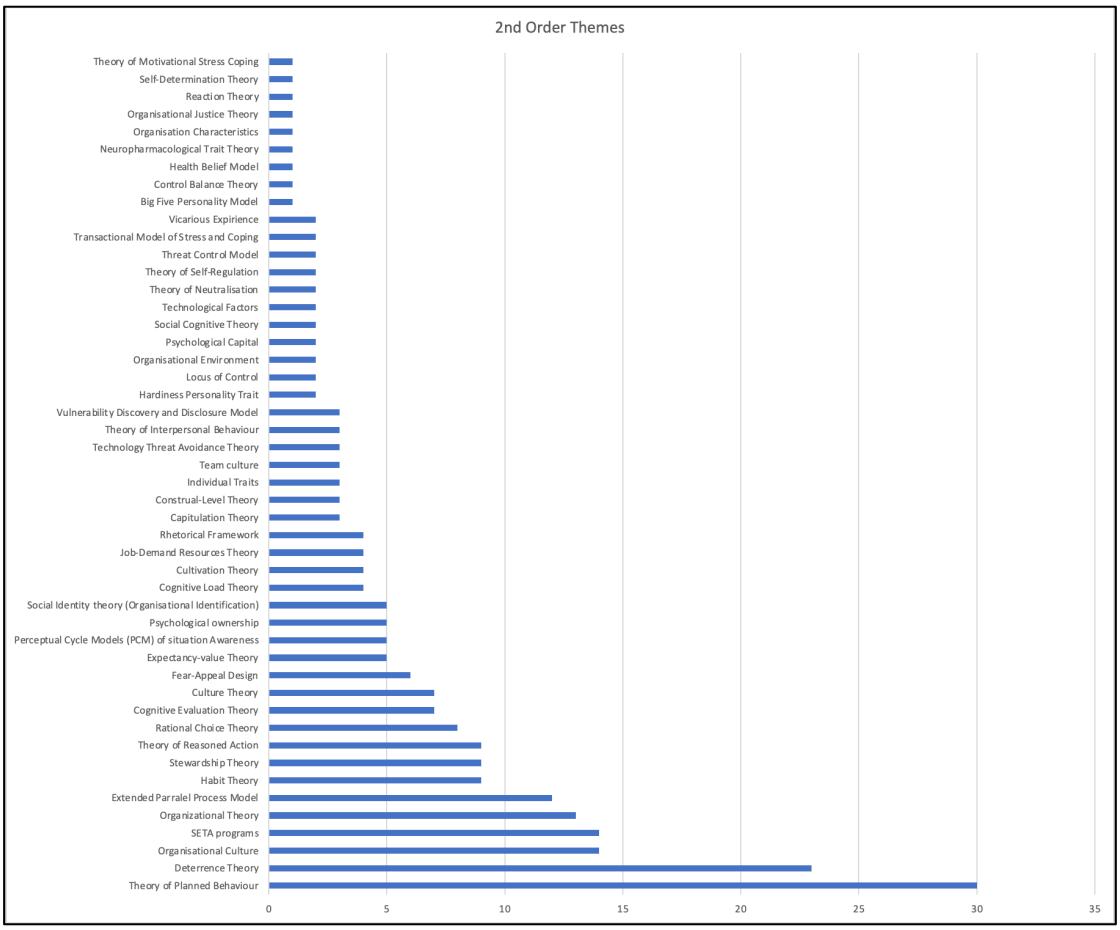


Adapted from (Gioia et al., 2012)

A total of 202 first-order constructs were coded in the literature analysed, with 22 of these constructs duplicated due to similarities between constructs across the theories, as also observed by (Moody et al., 2018). These constructs were grouped into 49 second-order themes and further grouped into eight overarching dimensions. Many of the first-order constructs were used interchangeably between second-order themes, and as such, many themes are grouped into more than one group. Additionally, many first-order constructs were

orphaned and not grouped into second-order themes, but were instead directly grouped into dimensions.

Figure 11 - Main Theories/Frameworks/Models



Source: Author

Figure 11 shows the frequencies of second-order codes applied to the literature using Atlas.ti (2025).

48 models, frameworks and theories were observed, which extended the Protection Motivation Theory to study users' information security behaviour from 2008 to 2025. The top 10 theories identified are: 1) Theory of Planned Behaviour, 2) Deterrence Theory, 3) Organisational Culture, 4) Security Education, Training and Awareness (SETA) and 5) Organisational Theory. These five theories account for 38% of the total theories that extend the Protection Motivation Theory.

Listing the frequency of the main second-order themes and grouping them offers little insight into how the Protection Motivation Theory was extended. Further, it highlights the scattered nature of the domain. Although depicting the more prominent second-order themes, no clear pattern can be observed.

Leach (2003) categorises user information security behaviour into 1) difficulty following security policies, 2) informal psychological contracts, 3) users' values and beliefs, 4) senior management and peer behaviour, 5) users' cognitive abilities and decision-making, and 6) organisational communication on expected behaviours. Balagopal and Mathew (2024) proposed the categorisation of the prevalent theories they observed influencing users' propensity to violate or comply with organisational information security policies.

An overlay of these categories was used, amended, and extended to group second-order themes into the overall overarching dimensions. The categories posited by Leach (2003), namely user values, beliefs, decision-making, difficulty following policies, and cognitive ability, were consolidated into Conscious Decision-Making. The informal psychological contract and management support were consolidated into the Social and Organisational dimensions. Lastly, organisational communication was consolidated into Rhetoric and Communication.

From the groups proposed by Balagopal and Mathew (2024), their organisational factor grouping informed the categorisation of second-order themes, and extended this with additional social and cultural theories observed. This was named the Social and Organisational group. Their individual-level decision-making group informed the grouping of second-order themes related to individual decision-making. This group was renamed to Cognitive Decision Making to reflect the cognitive focus of some of the theories represented, for example, the Cognitive Load Theory (Sweller, 2019) and Cognitive Evaluation Theory (Deci et al., 1975).

The stress group observed by Balagopal and Mathew (2024) informed the grouping of second-order themes and was extended to include themes of emotion to reflect stress as a negative emotion (Zhen et al., 2021). This group was named Emotional and Stress. The neutralisation and deterrence grouping proposed by scholars was consolidated into the Cognitive Decision Making group because of the cognitive process of justification of wrongdoing posited by the Neutralisation Theory (Sykes & Matza, 1957), and weighing the

pros and cons before deciding to act maliciously, as explained by the Deterrence Theory (Siponen & Vance, 2010).

Shiau et al. (2023) did a citation analysis of the trends in information security and found security decision making and management to be a prevalent theme, and as such, informed the grouping of cognitive and decision-making dimension.

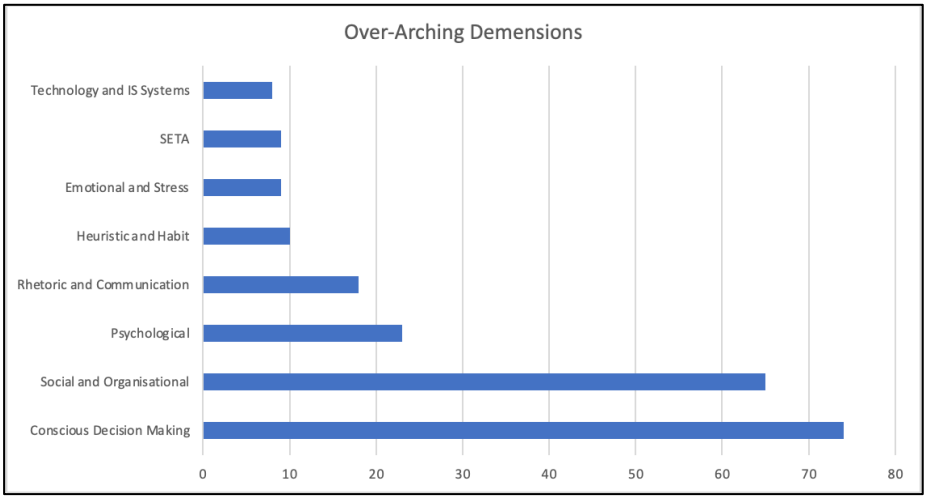
During the analysis, five additional dimensions were observed. These include Psychological, Rhetorical, and Communications dimensions, Technology and IS Systems dimensions, Heuristics and Habit dimensions, and Security Education, Training, and Awareness dimensions.

The final dimensional grouping is 1) Dimension 1 - Cognitive Decision Making, 2) Dimension 2 - Social and Organisational, 3) Dimension 3 – Psychological, 4) Dimension 4 - Emotional and Stress, 5) Dimension 5 - Rhetoric and Communications, 6) Dimension 6 - Technology and IS systems, 7) Dimension 7 - Heuristic and Habit, and 8) Dimension 8 - Security Education, Training and Awareness (SETA).

Figure 12 shows the grouping and frequency of codes in the literature analysed. The basis of Behavioural Information Security, using Protection Motivation Theory, is primarily built on constructs, themes, theories, models, and frameworks that encompass cognition, decision-making, social, and organisational dimensions.

As the search for the studies explicitly set out to gather studies using Protection Motivation Theory, which is a cognitive processing theory according to Rogers (1983); and based within a work setting, these results were to be expected.

Figure 12 - Dimensions of extant research



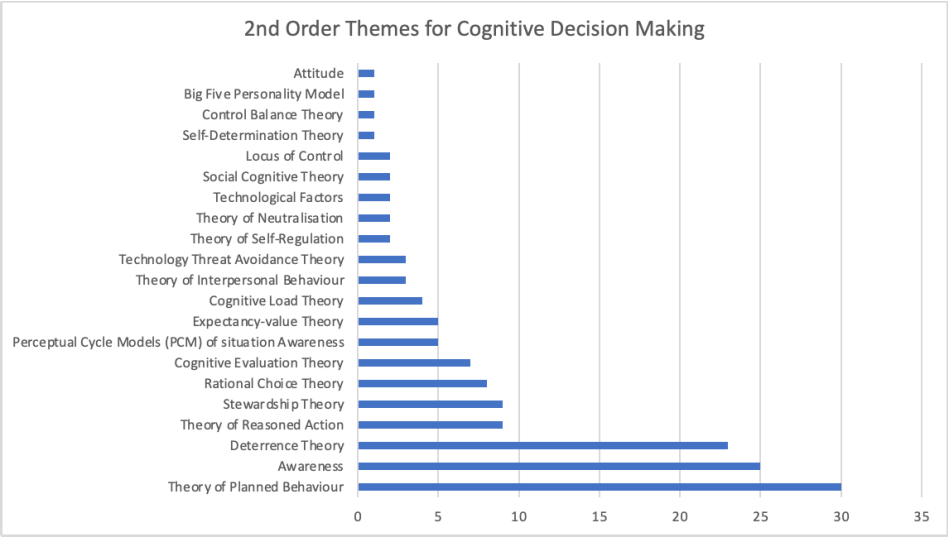
Source: Author

The following section details the eight dimensions, outlining the main theories, models, constructs, and frameworks observed. The figures show the frequency of these in the literature analysed.

3.2.1 Dimension 1 - Cognitive Decision Making

This dimension is the most observed in the literature analysed. It groups the themes that explain the cognitive decision-making theories used to study users' information security behaviour. Figure 13 illustrates the themes and constructs that comprise the dimension.

Figure 13 - Cognitive Decision-Making Dimension



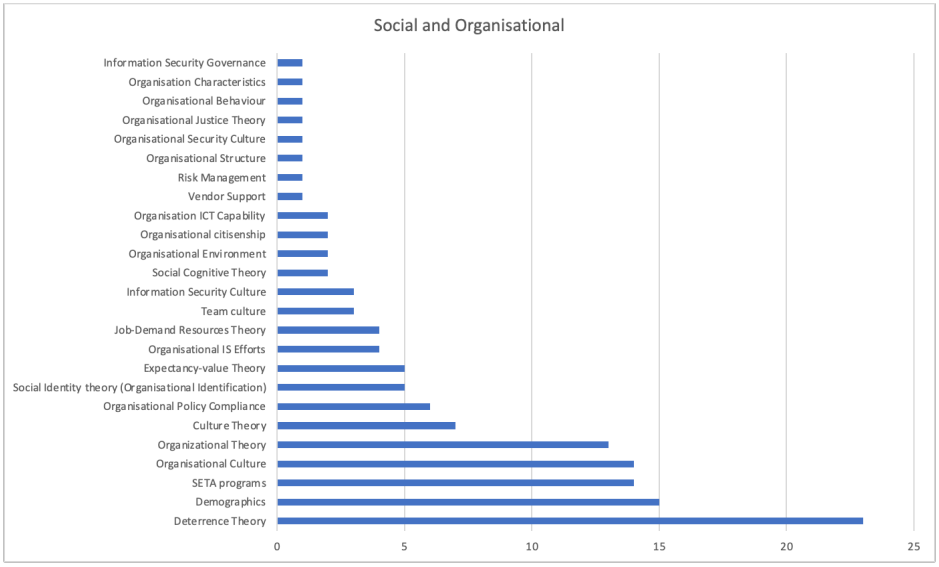
Source: Author

The Theory of Planned Behaviour and Deterrence Theory was this dimension's most used theoretical perspective. Awareness was identified as a key construct.

3.2.2 Dimension 2 - Social and Organisational

The second most prevalent dimension was the Social and Organisational dimension. This dimension focuses on the influence organisational and social factors such as organisational culture, governance and job demands has on a user's information security behaviour. Deterrence Theory remains the most used theory to explain organisational efforts to inspire positive information security behaviours. Demographical factors such as education levels, age of employees and gender has also been used to study employee's information security behaviour. Security Education, Training and Awareness, which also has a separate domain, is also list as an organisational factor that influences user information security behaviour.

Figure 14 - Social and Organisational Dimension

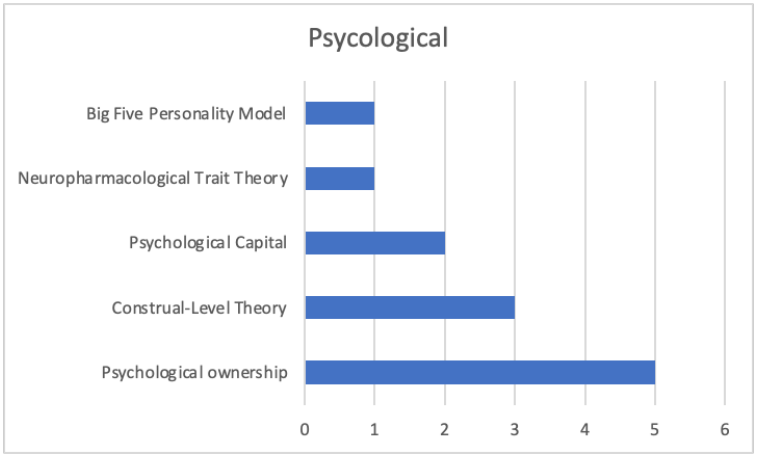


Source: Author

3.2.3 Dimension 3 - Psychological

An emerging dimension from the literature analysed is use of psychological theories to study user information security behaviour. Psychological ownership is the main construct in the dimension. Beyond user information security behaviour, Oakley et al. (2020) had argued that psychological ownership be integrated into the Protection Motivation Theory to understand protection motivation in the housing industry. Its importance can be noted from this review. Personality was also observed as an indicator of user information security behaviour.

Figure 15 - Psychological Dimension

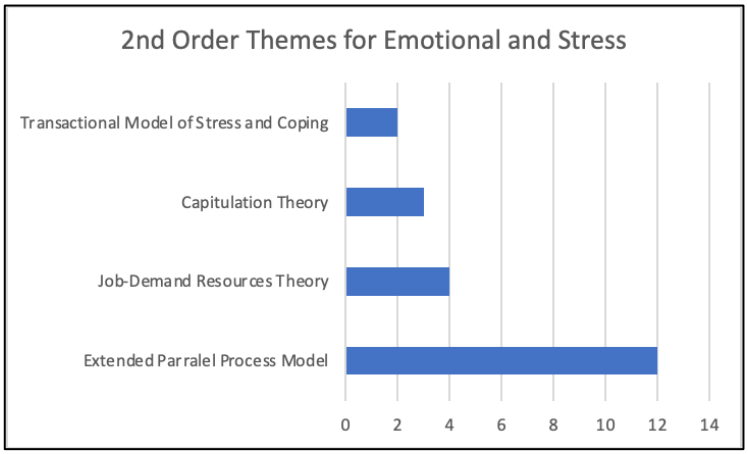


Source: Author

3.2.4 Dimension 4 - Emotional and Stress

The Extended Parallel Process Model is the most prevalent second-order theme in this dimension. This model is argued to be a suitable lens for studying user information security behaviour because it can depict both emotional and cognitive factors, with fear mediating between a defensive or protective motivation (Chen et al., 2021). The remainder of the theories and models are less prevalent in the extant literature.

Figure 16 – Emotional and Stress Dimension



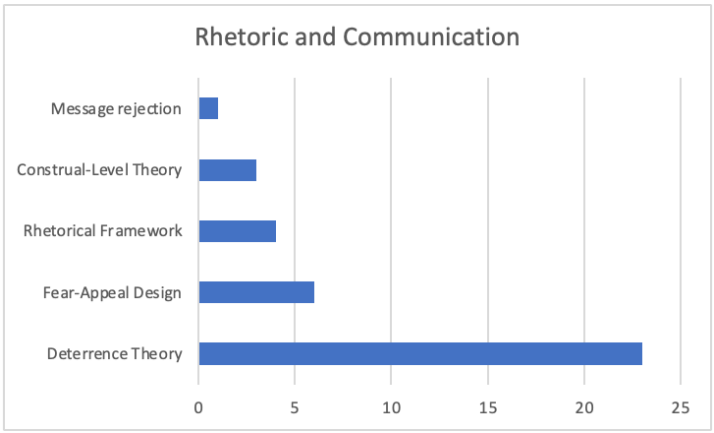
Source: Author

3.2.5 Dimension 5 - Rhetoric and Communication

This dimension group themes depicting models used to understand the effectiveness of communication methods in influencing user information security behaviour. Deterrence Theory is also present in this group because of the communication aspect of the theory. The

remainder of the constructs and theories observed describe how information security messaging was studied, from its design and applicability to the audience, as well as message rejection or acceptance.

Figure 17 – Dimension 5 – Rhetoric and Communication

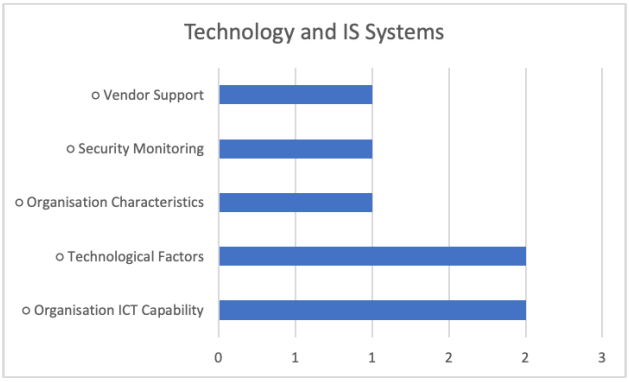


Source: Author's Own

3.2.6 Dimension 6 - Technology and IS systems

This dimension encompasses constructs such as the technological mechanism for monitoring users, organisational characteristics like reliance on information systems, and other technological factors, including investment in technology and vendor support, as shown in Figure 18.

Figure 18 - Technology and IS Systems

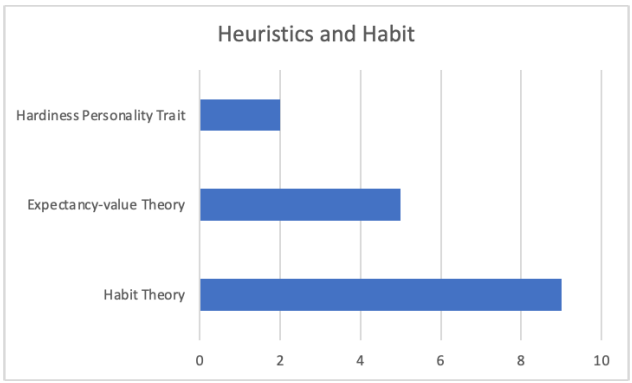


Source: Author

3.2.7 Dimension 7 - Heuristics and Habit

The Habit Theory is the most used in this dimension. Habit is described as routine behaviour based on past experiences and is set to influence user information security behaviour (Vance et al., 2012). Figure 19 outlines the constructs of Dimension 7.

Figure 19 – Heuristic and Habit Dimension

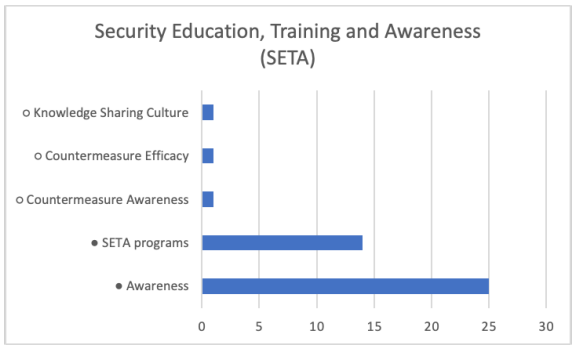


Source: Author

3.2.8 Dimension 8 - Security Education, Training and Awareness (SETA).

This dimension, as shown in Figure 20, describes the emphasis that extant literature places on education, training and awareness to inform users of the potential impact that an information security breach can have on the organisation. This dimension shares constructs like culture and awareness with dimensions 1 and 2, and awareness forms the basis of this dimension. It also highlights the focus the literature has on SETA programs within organisations.

Figure 20 – Security Education, Training and Awareness (SETA)



Source: Author's Own

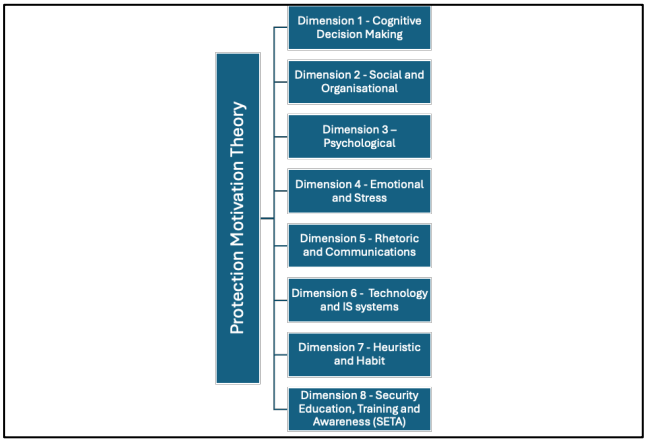
3.3 Summary of Section 3

This section displays the frequency of publications in the field and the annual publication rate. The journals and their respective ranking are described, highlighting SCImago Journal and Country Rank (SJR) indicators Q1-ranked journals were the most prevalent in the literature analysed.

The rate of publications per journal per year is shown, with the top five journals listed. The geographic location of the research focus is indicated, with the top country highlighted.

Section 3.2 discusses the analysis and coding results, outlining the overlaying grouping process adapted from the extant literature to inform the grouping of second-order and dimensional variables. The dimensions are defined and discussed. Figure 21 summarises the eight dimensions

Figure 21- Summary of Extension of Protection Motivation



Source: Author's Own

The section detailed the findings of each respective dimension, laying the foundation for the synthesis in the following section, Section 4.

4. Section 4: Synthesis of the Literature Review

Although the Protection Motivation Theory is limited in explaining users' behaviours to only reflecting a cognitive process, it is shown to be flexible in incorporating with other constructs, models, theories, and frameworks. This allows scholars to gain an expansive overview of users' behaviour in specialised or nuanced contexts where the Protection Motivation theory is lacking.

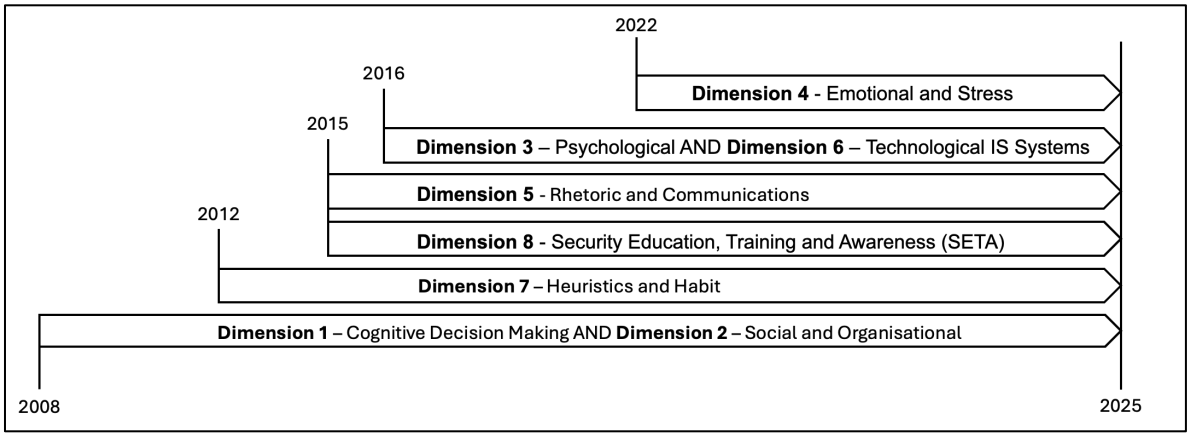
The eight dimensions described in the previous sections demonstrate how the Protection Motivation Theory has been extended into specialised areas, each requiring a focused theoretical lens.

The following section describes the evolution of the dimensions identified in the previous section to understand the tenure of these dimensions within the field. The subsequent section then details the frequency of these dimensions from 2008 to demonstrate where more scholarly work may be required, while highlighting areas where maturity may have been reached and areas of possible stagnation.

4.1 The evolution of PMT extension – 2008 to 2025

This section demonstrates the evolution of the various dimensions discussed previously. Figure 22 shows a timeline outlining the emergence of each of the eight domains in the literature analysed.

Figure 22 - Evolution of Dimensions since 2008



Source: Author's own

Through the lens of Protection Motivation Theory, the literature in the field is built on two dimensions: Dimension 1 – Cognitive Decision Making and Dimension 2 – Social and Organisational. The two dimensions are the foundation of scholarship in the field. The first study in the analysis employs the Protection Motivation Theory as the basis for examining the internal and external locus of control, aiming to understand why users continue to act in a contradictory manner, even when they are well-informed about what to do when faced with an information security threat (Workman et al., 2008).

Dimensions 1 and 2 are observable in the literature throughout, but in 2012, Vance et al. (2012) proposed the inclusion of habit as a factor to understand user information security behaviour. This led to the expansion of the field into Dimension 7 – Heuristics and Habit. This dimension argues that behaviour cannot be understood solely through cognitive measures, but must also account for automatic human behaviour (Vance et al., 2012). The scholars demonstrated the influence of habit on users' coping and threat appraisals, affecting their behaviour. Although the work of Vance et al. (2012) introduced a novel way to study users' information security behaviour, adoption in to the field was slow and could only be observed again in 2021 (Shahbaznezhad et al., 2021) and 2022 (Aigbefo et al., 2022).

In 2015, the field expanded its understanding of the role of education, communication, and awareness in user information security behaviour, thereby introducing Dimension 8 – Security Education, Training, and Awareness (SETA) and Dimension 5 – Rhetoric and Communication. Posey et al. (2015) and Safa et al. (2015) focused their research on expanding the field further into the Security Education, Training and Awareness (SETA) dimension, where they highlighted the importance of user awareness as a critical factor in affecting users overall information security behaviour.

Expanding on Dimension 5 – Rhetoric and Communication, Johnston et al. (2015) considered the influence of organisational communication rhetoric in informing users of the importance of behaving in a manner conducive to information security. This study paved the way for novel approaches to how organisations can design vignettes to effectively communicate and possibly overcome the concerns raised by scholars about the lack of personal relevance users may feel towards securing organisational information, as noted by Sommestad et al. (2015b).

Although Dimension 8 - Security Education, Training and Awareness (SETA) was regularly observed in the literature analysed through the awareness construct, Dimension 5 – Rhetoric and Communication remained rather dormant until 2020, where Schuetz et al. (2020) proposed that the level of abstraction in information security communication vignettes influences users information security behaviour. Schuetz et al. (2021) further expanded this dimension positing that information security messaging to users requires a component that deals with how and why to avert an information security threat.

As the field began to gain traction post 2015, a shift towards Dimension 3 – Psychological and Dimension 6 – Technological IS Systems is observed. Johnston et al. (2016), Burns et al. (2017) and Menard et al. (2018) included constructs like psychological capital, positive psychology, psychological ownership and personality to extend the discourse into Dimension 3. This dimension examines user dispositional and situational factors, the effect of hope, resilience and optimism and a user's sense of ownership to enhance their overall information security behaviour.

Furthermore, Yang and Lee (2016), Hovav and Putri (2016), and Torten et al. (2018) further expanded the field to include technological factors like investment in technology solutions, the organisation's overall reliance on technology, monitoring solutions and overall technology use, thereby extending the field into Dimension 6.

Although not considered a dimension in the review, the efforts by scholars to unify the models used to study users' information security behaviour are notable in the evolution of the field. Scholars observed the disparate theories, models, constructs, and frameworks used to study user information security behaviour and believed it was best to create a shared basis for Behavioural Information Security research. Chen et al. (2018) and Moody et al. (2018) attempted to conceptualise a unifying model that incorporates constructs from the lenses used in literature. The scholars encouraged harmonisation of the field through the application of a unified model to study user information security behaviour. Their respective models mainly borrowed from various theories and models, but more importantly, both scholars emphasised the significance of Dimension 7 and 8, with Chen et al. (2018) highlighting the importance of SETA and Moody et al. (2018) calling for further research into the habit domain.

Additionally, an interesting observation around 2018 was the inclusion of the Technology Threat Avoidance Theory in some of the studies analysed. This theory was initially

suggested by Liang and Xue (2009) to explain users' behaviour in response to information technology threats. What is interesting is the similarities that this theory shares with the Protection Motivation Theory. The theory is described as the Protection Motivation Theory applied to Information Security (Moody et al., 2018), a Protection Motivation Theory-like theory that borrows from the Protection Motivation Theory (Sreenath et al., 2025; Vrhovec & Mihelič, 2021), and shares foundational elements and theories (McLeod & Dolezel, 2022).

The emergence of the Technology Threat Avoidance Theory in the literature indicates that scholars have recognised the importance of evolving and localising adaptive theories such as the Protection Motivation Theory, which was initially adopted from the health domain to the field of Behavioural Information Security. Despite this, scholars have not sufficiently explored the theory as its prevalence in the literature analysed remains limited, as shown by Figure 11.

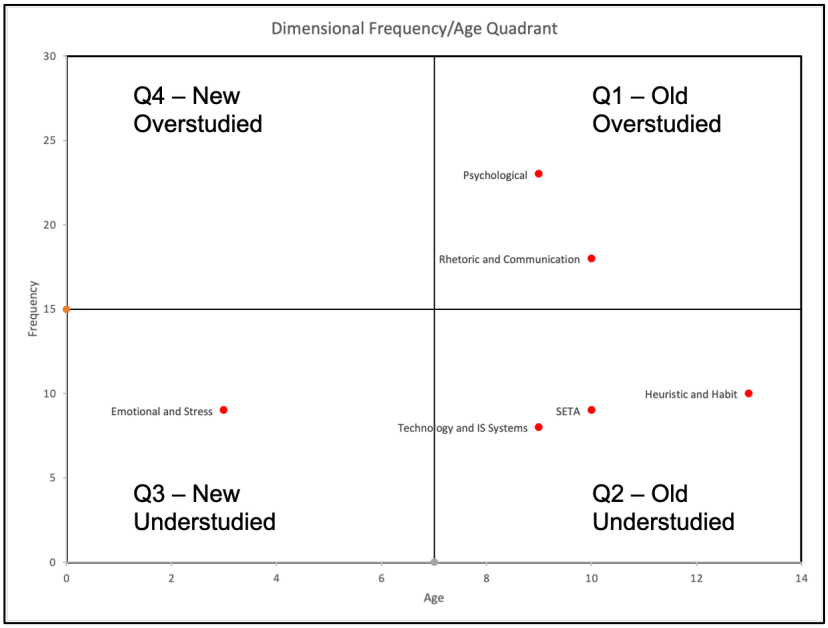
The field remained relatively stagnant within Domain 1 and 2, few studies branching out into the Dimension 3 - Psychology, Dimension 6 – Technology and IS Systems, Dimension 5 – Rhetoric and Communication and Dimension 7 – Heuristics and Habit. Although many studies during this time used the Extended Parallel Process Model, as shown in Dimension 4 – Emotional and Stress, none considered the more niche constructs observed in later studies. In 2022, however, McLeod and Dolezel (2022) introduced the concept of capitulation as a construct that can be studied to understand users' information security behaviour. This opened the field to the emotional and stress domain, which has gained interest in the past few years. Kim et al. (2024) and Aggarwal and Srivastava (2024) introduced the concept of job-related stress and eustress, respectively, further expanding the domain.

The field of Behavioural Information Security, particularly in the context of Protection Motivation Theory as a prime lens, has expanded into eight dimensions from 2008 to 2025. This evolution, coupled with the growth of the published literature described in Section 3.1, shows that interest in the field is growing.

4.2 Dimension Age/Frequency Analysis

An analysis of the prevalence of the dimensions used in literature from 2008 to 2025 against their tenure in the field was conducted. Four quadrants were used: Q1 – Old Overstudied Dimensions, Q2 – Old Understudied Dimensions, Q3 – New Understudied Dimensions, and Q4 – New Overstudied Dimensions. Dimensions 1 and 2 were omitted as they were found to be the basis of the field and may not offer any deeper understanding when included in the analysis. As such, only the remaining five dimensions were included in this part of the analysis.

Figure 23 - Dimensional frequency and Age Analysis



Source: Author's Own

Figure 23 illustrates the four quadrants, each representing one of the five dimensions against the age (in years) of the dimension in the field and its frequency or prevalence in the analysed literature. An interesting picture starts to emerge, where Dimension 7 – Heuristics and Habit, Dimension 8 - Security Education, Training and Awareness (SETA) and Dimension 6 – Technology and IS Systems form part of older dimensions in the field that have been understudied.

Dimensions 5—Rhetoric and Communication and Dimension 3—Psychological are some of the older dimensions in literature but have remained understudied for their time in the field.

Although Dimension 4 – Emotional and Stress is the newest dimension among the others, it has garnered significant scholarly attention. Dimension 6 – Technology and IS Systems has remained the most understudied dimension, and this could be attributed to the narrative that technology alone cannot successfully prevent information security breaches (Shiau et al., 2023).

The significance of performing this analysis lies in the observation of a distinction between the four quadrants, which delineates the frequency of the dimension as coded in Atlas.ti (2025), in comparison with its duration since it was first introduced in the literature analysed.

4.3 Synthesis with extant literature

Balagopal and Mathew (2024) offers a strong foundation for the current review, providing a lens through which the second-order themes can be grouped, as such informing the categorisation of this review. This review, however, differs from this work in that it employs an anchoring theory to guide the synthesis of findings from existing empirical research, whereas Balagopal and Mathew (2024) does not prioritise a specific theory. In addition, this review extends on the categorisation offered by the authors to include emergent dimensions.

Although this review consults the work of Leach (2003) to inform the grouping of first and second order themes, it distinguishes itself by employing a strong theoretical foundation, whereas Leach (2003) did not use a theoretical lens to inform their catagorisation, as posited by Anderson and Agarwal (2010).

Existing research on user information security behaviour has been characterised as disjointed and often contradictory. This review's findings align with those of scholars such as Cram et al. (2019) and Mou et al. (2022) in that the Behavioural Information Security field remains fragmented, considering the erratic use of various theories observed, as discussed in Section 3.2. This review aimed to understand how a common theory used in literature was applied to study users' information security behaviour within the context of various organisations, thereby consolidating disparate literature.

Previous reviews have highlighted the inconsistencies in the applicability of Protection Motivation Theory in explaining users' information security behaviours and argued for using other theories instead (Cram et al., 2019). This review shows that the Protection Motivation Theory has a solid foundation in Behavioural Information Security, especially within an organisational context. As such, this review aligns with the findings of Mou et al. (2022) in

that the theory may apply to an organisational setting and offers a solid theoretical basis for further studies. Furthermore, this review builds on the work of Shiau et al. (2023) by expanding on their security decision-making and management by extending the key constructs observed by the scholars.

The use of a prime theoretical foundation as a lens through which existing literature is reviewed offers a novel perspective through which efforts can be focused to consolidate disjoint findings. This review proposes eight overarching dimensions grounded in a single theory and contributes to the scholarship by mapping the existing domains and illustrating their evolution over time.

Furthermore, through the coding analysis conducted in Section 3.2, the review identified more prevalent dimensions and potential areas for future research. As such, the pressing need for a better understanding of the factors influencing users' information security behaviour to curb breaches can be addressed by perusing these dormant and understudied dimensions.

4.4 Summary of Section 4

Section 4 highlighted the evolution of the extension of Protection Motivation Theory within Behavioural Information Security. It was noted that the overall listing of theories and constructs provided little value to the review, and it was deemed prudent to understand how Protection Motivation Theory evolved over this period.

The frequency and age of the respective dimensions highlighted in the previous section were divided into quadrants to understand a dimension's tenure in relation to its prevalence in the literature studied. This offered insight into the over- and under-studied dimensions in the literature, delineating potential areas for future investigation.

Furthermore, the section highlighted areas where Behavioural Information Security may be experiencing stagnation. Dimension 7 – Heuristics and Habit has shown the longest tenure in the field; however, it has been relatively understudied compared to Dimension 5—Rhetoric and Communication and Dimension 3—Psychological. This might suggest that interest in this dimension has diminished.

Focusing on Dimension 5—Rhetoric and Communication and Dimension 3—Psychological demonstrates that the dimensions have been in the field for nine and ten years, respectively. These dimensions have garnered the most attention in the field.

The section also highlights Dimension 4—Emotional and Stress—as an emergent dimension that has gained the most attention for its tenure in the field. It proceeds to synthesise this review's findings with the existing literature, comparing its results with those of other prominent studies in the field.

5. Section 5: Formulated Research Questions for Future Research and Conclusion

Information security breaches have become increasingly prominent, and their impact has become increasingly severe. The role users play in safeguarding organisational information has become more critical as users are regarded as both the cause and solution to information security breaches. This has sparked interest among scholars and practitioners alike, resulting in many studies aimed at understanding the factors that influence and motivate users to act in ways that prioritise organisational information security.

Although offering valuable insights, the field of Behavioural Information Security has established a sturdy base; however, it has been plagued by disparate findings and a lack of consistency. As such, scholars' ability to adequately explain and address user behaviour to improve security issues is severely hampered, especially in nuanced settings.

This review synthesised findings from the extant literature to strengthen the basis for future research. It consolidated research under a common theoretical lens, allowing a well-studied theory to provide a basis for understanding how it has been extended to explain specific or specialised areas.

Using the PRISMA process, the review searched for eligible literature from credible academic sources, employing well-defined search criteria, and then sifted through numerous reputable studies using an iterative selection process. A final batch of 60 studies was identified and analysed through a structured coding process, identifying first and second-order constructs.

Listing and arranging these constructs according to their prevalence in literature offered limited insights and necessitated further analysis by grouping these second-order themes into over-arching dimensions. Eight dimensions were identified, which emphasise how the Protection Motivation Theory was extended to enhance the understanding of user information security behaviour in an organisational setting.

5.1 Answering the review question

The eight dimensions described are integral to answering the review question, and, in doing so, highlight the areas for potential scholarship. The Protection Motivation Theory was extended into eight dimensions to study users’ information security behaviour. Answering this question also provided a basis for consolidating disparate findings in the field.

Additionally, this answer addresses the potential gap in knowledge where overemphasised, stagnated, and understudied areas can be identified to aid scholars and practitioners in understanding how to motivate users better to enhance organisational information security.

5.2 Theoretical Implications

It became clear during the analysis of existing literature that a single overarching theory, model, or framework may not address the eclectic field of Behavioural Information Security. As such, and not disregarding the contributions of scholars like Moody et al. (2018) and Chen et al. (2021), the field appears to be more adequately studied by integrating various lenses, curtailing the need for further research into such endeavours as posited by Cram et al. (2019). Although this review aligns with Cram et al. (2019) this view may not be as straightforward as argued by scholars.

Secondly, the emergence of the Technology Threat Avoidance Theory alongside the Protection Motivation Theory indicates that a comprehensive theory for understanding the factors that influence users' information security behaviour can be developed by combining these theories, considering the guidelines proposed by Okhuysen and Bonardi (2011) for integrating theories.

Lastly, an analysis of the evolution of various literary dimensions highlights their tenure in the field. However, comparing this with their prominence reveals gaps where potential scholarly attention may be required, as well as areas where further attention may yield limited findings. Additionally, this review highlights areas where potential stagnation is observed.

5.3 Practical Implications

This review highlights the importance of organisations investing more resources in understanding, managing, and motivating users to behave in a manner that promotes information safeguarding. Dimension 4—Emotional and Stress has highlighted the impact of work-related stress and the influence of fear on users' behaviour. Although it is a relatively new dimension in the field, its uptake as a key dimension of interest suggests its potential influence in the field compared to the other dimensions.

Secondly, the prominence of Dimension 7 – Heuristics and Habit and Dimension 5—Rhetoric and Communication underscores the importance for organisations to focus on

instilling good information security habits in their users and consider the influence that effective information security communication has on improving user behaviour.

The infrequent use of Dimension 6 – Technology and IS Systems indicates an area with limited studies that bridge the gap between technology and user information security behaviour. This aligns with the discourse prioritising user and organisational factors over technological ones in enhancing information security (Shiau et al., 2023). Addedly, the low frequency of Dimension 8 - Security Education, Training and Awareness (SETA) shows that training users, although effective in raising awareness among them, is given lower priority in literature. This could be because users continue to behave in a contradictory manner even when adequately trained (Chen et al., 2021).

5.4 Directions for future Research

As shown in section 4, Dimension 4—Emotional and Stress is an area with the most potential for future research. Fear, as an emotional response to threats, as discussed by Rogers (1983) and advocated by Boss et al. (2015) to enhance users' behaviour, still has potential for future research. Although much has already been done in this dimension, the emotional and stress dimension may offer future studies a strong foundation. In light of the growing information security threats to organisations that exploit emotional vulnerabilities and fallibility, it may be prudent to continue exploring this dimension.

Furthermore, continuing to focus on stagnant or mature dimensions may further delay any significant findings in the field, thereby hampering the ability to address current information security challenges adequately.

Secondly, the emergence of the Technology Threat Avoidance Theory as a Protection Motivation Theory-like theory specifically adapted to the information security field has offered a potential future avenue for researchers. Researchers may explore how this theory can be integrated with the Protection Motivation Theory, or how the Technology Threat Avoidance Theory has been extended in the existing literature to examine users' information security behaviour.

Lastly, the advent of malicious artificial intelligence to aid in exploiting user fallibility may prompt the development of additional dimensions. The non-existence of dimensions that explore how organisations address the rise of artificial intelligence as a tool to enhance

users' information security behaviour holds potential for future scholarly attention. Such analysis may require the inclusion of nudging and behavioural economics to improve users' information security behaviour, as explored by Inaba and Terada (2023). Furthermore, building on the work of Schmitt and Flechais (2024) may provide the basis for using Protection Motivation Theory to examine the development of secure user behaviour using Artificial Intelligence.

5.5 Study Limitations

Although reasonable attention has been given to ensure the completeness of the current review, limitations are inevitable. The review only focused on English-based studies, which may have limited its reach. As such, future research could focus on extending the findings in the field by investigating research in other languages.

Additionally, the limited availability of scholarly databases and published articles restricted the research to an academic perspective, without considering the potential views of practitioners. Considering the cross-dimensional reach of Behavioural Information Security between academia and practice, it may be prudent for future reviews to incorporate grey literature to synthesise both perspectives.

Lastly, the exclusion of lower-ranked journals from the review may have limited the reach of these findings. Although the journal's ranking is an indication of the quality of research published therein, many insightful or impactful research studies may not be published there due to other factors (Osterloh & Frey, 2020). As such, this review may have overlooked relevant literature that could have contributed to the findings presented.

5.6 Declaration of A.I use

Grammarly A.I was used to assist in ensuring the grammatical accuracy and coherent sentence construction of the review. ChatGPT was used to assist with the design of Figure 7, utilising the data provided by the Author.

6. References

Aggarwal, A., & Srivastava, S. K. (2024). Exploring eustress and fear: A new perspective on protection motivation in information security policy compliance within the financial sector. *Computers & Security*, *142*. https://doi.org/10.1016/j.cose.2024.103857

Aigbefo, Q. A., Blount, Y., & Marrone, M. (2022). The influence of hardiness and habit on security behaviour intention. *Behaviour & Information Technology*, *41*(6), 1151-1170. https://doi.org/10.1080/0144929x.2020.1856928

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

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*(3), 613-643. https://doi.org/10.2307/25750694

Atlas.ti. (2025). (Version 25.0.1 (32922)) ATLASti Scientific Software Development GmbH.

Balagopal, N., & Mathew, S. K. (2024). Exploring the factors influencing information security policy compliance and violations: A systematic literature review. *Computers & Security*, *147*. https://doi.org/10.1016/j.cose.2024.104062

Bayl-Smith, P., Taib, R., Yu, K., & Wiggins, M. (2022). Response to a phishing attack: Persuasion and protection motivation in an organizational context. *Information & Computer Security*, *30*(1), 63-78. https://doi.org/10.1108/ICS-02-2021-0021

Bélanger, F., Maier, J., & Maier, M. (2022). A longitudinal study on improving employee information protective knowledge and behaviors. *Computers & Security*, *116*. https://doi.org/10.1016/j.cose.2022.102641

Beller, E. M., Glasziou, P. P., Altman, D. G., Hopewell, S., Bastian, H., Chalmers, I., Gøtzsche, P. C., Lasserson, T., & Tovey, D. (2013). Prisma for abstracts: Reporting systematic reviews in journal and conference abstracts. *PLoS Medicine*, *10*(4), e1001419. https://doi.org/10.1371/journal.pmed.1001419

Boss, S. R., Galletta, D. F., Benjamin Lowry, P., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, *39*(4), 837 - 864. https://uplib.idm.oclc.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=110877517&site=ehost-live&scope=site

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523-A527. https://doi.org/10.2307/25750690

Burns, A. J., Posey, C., Roberts, T. L., & Benjamin Lowry, P. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, *68*, 190-209. https://doi.org/10.1016/j.chb.2016.11.018

Chen, X., Chen, L., & Wu, D. (2018). Factors that influence employees' security policy compliance: An awareness-motivation-capability perspective. *Journal of Computer Information Systems*, *58*(4), 312-324. https://doi.org/10.1080/08874417.2016.1258679

Chen, Y., Galletta, D. F., Lowry, P. B., Luo, X., Moody, G. D., & Willison, R. (2021). Understanding inconsistent employee compliance with information security policies through the lens of the extended parallel process model. *Information Systems Research*, *32*(3), 1043-1065. https://doi.org/10.1287/isre.2021.1014

Corley, K. G., & Gioia, D. A. (2004). Identity ambiguity and change in the wake of a corporate spin-off. *Administrative Science Quarterly*, *49*(2), 173-208. https://doi.org/10.2307/4131471

Crabtree, B. F., & Miller, W. F. (1992). A template approach to text analysis: Developing and using codebooks. In *Doing qualitative research.* (pp. 93-109). https://research.ebsco.com/linkprocessor/plink?id=dd4b2fe6-2260-3b93-a1c6-2f30f161bd02

Cram, W. A., D'Arcy, J., & Benlian, A. (2024). Time will tell: The case for an idiographic approach to behavioral cybersecurity research. *MIS Quarterly*, *48*(1), 95-136. https://doi.org/10.25300/misq/2023/17707

Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, *43*(2), 525-554. https://doi.org/10.25300/misq/2019/15117

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90-101. https://doi.org/10.1016/j.cose.2012.09.010

Dalal, R. S., Howard, D. J., Bennett, R. J., Posey, C., Zaccaro, S. J., & Brummel, B. J. (2022). Organizational science and cybersecurity: Abundant opportunities for research at the interface. *J Bus Psychol*, *37*(1), 1-29. https://doi.org/10.1007/s10869-021-09732-9

Deci, E. L., Cascio, W. F., & Krusell, J. (1975). Cognitive evaluation theory and some comments on the calder and staw critique. *Journal of personality and social psychology*, *31*(1), 81-85. https://doi.org/10.1037/h0076168

Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2021). Human factors in phishing attacks: A systematic literature review. *ACM Computing Surveys*, *54*(8), 1-35. https://doi.org/10.1145/3469886

Dhillon, G., & Backhouse, J. (2001). Current directions in is security research: Towards socio-organizational perspectives. *Information Systems Journal*, *11*(2), 127-153. https://doi.org/10.1046/j.1365-2575.2001.00099.x

Dodge, C. E., Fisk, N., Burruss, G. W., Moule, R. K., & Jaynes, C. M. (2023). What motivates users to adopt cybersecurity practices? A survey experiment assessing protection motivation theory. *Criminology & Public Policy*, *22*(4), 849-868. https://doi.org/10.1111/1745-9133.12641

Fan, D., Breslin, D., Callahan, J. L., & Iszatt-White, M. (2022). Advancing literature review methodology through rigour, generativity, scope and transparency. *International Journal of Management Reviews*, *24*(2), 171-180. https://doi.org/10.1111/ijmr.12291

Fereday, J., & Muir-Cochrane, E. (2006). Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International Journal of Qualitative Methods*, *5*(1), 80-92. https://doi.org/10.1177/160940690600500107

Gerdin, M. (2025). Validating and extending the unified model of information security policy compliance. *Information and Computer Security*, *33*(1), 25-48. https://doi.org/10.1108/ics-12-2023-0263

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2012). Seeking qualitative rigor in inductive research. *Organizational Research Methods*, *16*(1), 15-31. https://doi.org/10.1177/1094428112452151

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems*, *18*(1), 22-44. https://doi.org/10.17705/1jais.00447

Gregor, S. (2006). The nature of theory in information systems. *MIS Quarterly*, *30*(3), 611-642. https://doi.org/10.2307/25148742

Gusenbauer, M., & Haddaway, N. R. (2020). Which academic search systems are suitable for systematic reviews or meta-analyses? Evaluating retrieval qualities of google scholar, pubmed, and 26 other resources. *Res Synth Methods*, *11*(2), 181-217. https://doi.org/10.1002/jrsm.1378

Hanus, B., & Wu, Y. A. (2015). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, *33*(1), 2-16. https://doi.org/10.1080/10580530.2015.1117842

Hemshorn de Sanchez, C. S., Gerpott, F. H., & Lehmann-Willenbrock, N. (2021). A review and future agenda for behavioral research on leader–follower interactions at different temporal scopes. *Journal of Organizational Behavior*, *43*(2), 342-368. https://doi.org/10.1002/job.2583

Hovav, A., & Putri, F. F. (2016). This is my device! Why should i follow your rules? Employees' compliance with byod security policy. *Pervasive and Mobile Computing*, *32*, 35-49. https://doi.org/10.1016/j.pmcj.2016.06.007

IBM. (2024). *Cost of a data breach report 2024*. https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95. https://doi.org/10.1016/j.cose.2011.10.007

Inaba, M., & Terada, T. (2023). *Nudge to promote employees' information security compliance behavior: A field study* 2023 IEEE International Conference on Cyber Security and Resilience (CSR),

Jansen, J., & van Schaik, P. (2019). The design and evaluation of a theory-based intervention to promote security behaviour against phishing. *International Journal of Human-Computer Studies*, *123*, 40-55. https://doi.org/10.1016/j.ijhcs.2018.10.004

Jeyaraj, A., & Zadeh, A. H. (2020). Evolution of information systems research: Insights from topic modeling. *Information & Management*, *57*(4). https://doi.org/10.1016/j.im.2019.103207

Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and situational factors: Influences on information security policy violations. *European Journal of Information Systems*, *25*(3), 231-251. https://doi.org/10.1057/ejis.2015.15

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework. *MIS Quarterly*, *39*(1), 113-134.

Karjalainen, M., Sarker, S., & Siponen, M. (2019). Toward a theory of information systems security behaviors of organizational employees: A dialectical process perspective. *Information Systems Research*, *30*(2), 687-704. https://doi.org/10.1287/isre.2018.0827

Kim, B.-J., Kim, M.-J., & Lee, J. (2024). Examining the impact of work overload on cybersecurity behavior: Highlighting self-efficacy in the realm of artificial intelligence. *Current Psychology*, *43*(19), 17146-17162. https://doi.org/10.1007/s12144-024-05692-4

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

Leach, J. (2003). Improving user security behaviour. *Computers & Security*, *22*(8), 685-692. https://doi.org/10.1016/s0167-4048(03)00007-5

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & H. Breitner, M. (2014). Information security awareness and behavior: A theory-based literature review. *Management Research Review*, *37*(12), 1049-1092. https://doi.org/10.1108/MRR-04-2013-0085

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. *Behaviour & Information Technology*, *27*(5), 445-454. https://doi.org/10.1080/01449290600879344

Li, H., Deng, Y., Huang, Y., & Blake, H. (2025). Predicting dietary management intention of patients with chronic kidney disease using protection motivation theory. *PLoS One*, *20*(3), e0320340. https://doi.org/10.1371/journal.pone.0320340

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, *33*(1), 71-90. https://doi.org/10.2307/20650279

Liang, N., Hirschheim, R., Luo, X., & Hollingsworth, H. (2023). Identifying the idiosyncrasies of behavioral information security discourse and proposing future research directions: A foucauldian perspective. *Journal of Information Technology*, *38*(4), 382-415. https://doi.org/10.1177/02683962231181146

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P., Clarke, M., Devereaux, P. J., Kleijnen, J., & Moher, D. (2009). The prisma statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: Explanation and elaboration. *Annals of internal medicine*, *151*(4), W-65-W-94.

Lowry, P. B., Moody, G. D., Parameswaran, S., & Brown, N. J. (2023). Examining the differential effectiveness of fear appeals in information security management using two-stage meta-analysis. *Journal of Management Information Systems*, *40*(4), 1099-1138. https://doi.org/10.1080/07421222.2023.2267318

McLeod, A., & Dolezel, D. (2022). Information security policy non-compliance: Can capitulation theory explain user behaviors? *Computers & Security*, *112*. https://doi.org/10.1016/j.cose.2021.102526

Menard, P., Bott, G. J., & Crossler, R. E. (2018). User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems*, *34*(4), 1203-1230. https://doi.org/10.1080/07421222.2017.1394083

Menard, P., Warkentin, M., & Lowry, P. B. (2018). The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. *Computers & Security*, *75*, 147-166. https://doi.org/10.1016/j.cose.2018.01.020

Mongeon, P., & Paul-Hus, A. (2015). The journal coverage of web of science and scopus: A comparative analysis. *Scientometrics*, *106*(1), 213-228. https://doi.org/10.1007/s11192-015-1765-5

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*(1), 285-311. https://doi.org/10.25300/misq/2018/13853

Mou, J., Cohen, J., Bhattacherjee, A., & Kim, J. (2022). A test of protection motivation theory in the information security literature: A meta-analytic structural equation modeling. *Journal of the Association for Information Systems*, *23*(1), 196-236. https://doi.org/10.17705/1jais.00723

Oakley, M., Mohun Himmelweit, S., Leinster, P., & Casado, M. (2020). Protection motivation theory: A proposed theoretical extension and moving beyond rationality—the case of flooding. *Water*, *12*(7). https://doi.org/10.3390/w12071848

Ogbanufe, O., Crossler, R. E., & Biros, D. (2023). The valued coexistence of protection motivation and stewardship in information security behaviors. *Computers & Security*, *124*. https://doi.org/10.1016/j.cose.2022.102960

Okhuysen, G., & Bonardi, J.-P. (2011). Editors' comments - the challenges of building theory by combining lenses. *Academy of Management Review*, *36*(1), 6-11. https://doi.org/10.5465/AMR.2011.55662498

Osterloh, M., & Frey, B. S. (2020). How to avoid borrowed plumes in academia. *Research Policy*, *49*(1). https://doi.org/10.1016/j.respol.2019.103831

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hrobjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S.,…Moher, D. (2021). The prisma 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, *372*, n71. https://doi.org/10.1136/bmj.n71

Park, J., Son, J.-Y., & Suh, K.-S. (2021). Fear appeal cues to motivate users' security protection behaviors: An empirical test of heuristic cues to enhance risk communication. *Internet Research*, *32*(3), 708-727. https://doi.org/10.1108/intr-01-2021-0065

Paul, J., Lim, W. M., O'Cass, A., Hao, A. W., & Bresciani, S. (2021). Scientific procedures and rationales for systematic literature reviews (spar-4-slr). *International Journal of Consumer Studies*, *45*(4). https://doi.org/10.1111/ijcs.12695

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), 179-214. https://doi.org/10.1080/07421222.2015.1138374

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors [Article]. *MIS Quarterly*, *37*(4), 1189-A1189. https://uplib.idm.oclc.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=91906245&site=ehost-live&scope=site

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

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social psychology: A source book*, 153-176.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65-78. https://doi.org/10.1016/j.cose.2015.05.012

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70-82. https://doi.org/10.1016/j.cose.2015.10.006

Sauer, P. C., & Seuring, S. (2023). How to conduct systematic literature reviews in management research: A guide in 6 steps and 14 decisions. *Review of Managerial Science*, *17*(5), 1899-1933. https://doi.org/10.1007/s11846-023-00668-3

Schmitt, M., & Flechais, I. (2024). Digital deception: Generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review*, *57*(12). https://doi.org/10.1007/s10462-024-10973-2

Schuetz, S. W., Benjamin Lowry, P., Pienta, D. A., & Bennett Thatcher, J. (2020). The effectiveness of abstract versus concrete fear appeals in information security. *Journal of Management Information Systems*, *37*(3), 723-757. https://doi.org/10.1080/07421222.2020.1790187

Schuetz, S. W., Lowry, P. B., Pienta, D. A., & Thatcher, J. B. (2021). Improving the design of information security messages by leveraging the effects of temporal distance and argument nature. *Journal of the Association for Information Systems*, *22*(5), 1376-1428. https://doi.org/10.17705/1jais.00697

Seini, A. B., Adam, I. O., & Alhassan, M. D. (2025). Examining the effect of security behaviour on the continuance use of mobile money services in ghana: A protection motivation perspective. *Information Technology for Development*, 1-18. https://doi.org/10.1080/02681102.2025.2483695

Seuring, S., Yawar, S. A., Land, A., Khalid, R. U., & Sauer, P. C. (2021). The application of theory in literature reviews – illustrated with examples from supply chain management. *International Journal of Operations & Production Management*, *41*(1), 1-20. https://doi.org/10.1108/IJOPM-04-2020-0247

Shahbaznezhad, H., Kolini, F., & Rashidirad, M. (2021). Employees' behavior in phishing attacks: What individual, organizational, and technological factors matter? *Journal of Computer Information Systems*, *61*(6), 539-550. https://doi.org/10.1080/08874417.2020.1812134

Shiau, W.-L., Wang, X., & Zheng, F. (2023). What are the trend and core knowledge of information security? A citation and co-citation analysis. *Information & Management*, *60*(3). https://doi.org/10.1016/j.im.2023.103774

Simmons, N. (2017). The sage encyclopedia of communication research methods. In. https://doi.org/https://doi.org/10.4135/9781483381411.n33

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487-A412. https://doi.org/10.2307/25750688

Siponen, M. T. (2000a). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31-41. https://doi.org/10.1108/09685220010371394

Siponen, M. T. (2000b). Critical analysis of different approaches to minimizing user-related faults in information systems security: Implications for research and practice. *Information Management & Computer Security*, *8*(5), 197-209. https://doi.org/10.1108/09685220010353178

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333-339. https://doi.org/10.1016/j.jbusres.2019.07.039

Sommestad, T., Karlzén, H., & Hallberg, J. (2015a). A meta-analysis of studies on protection motivation theory and information security behaviour. *International Journal of Information Security and Privacy*, *9*(1), 26-46. https://doi.org/10.4018/ijisp.2015010102

Sommestad, T., Karlzén, H., & Hallberg, J. (2015b). A meta-analysis of studies on protection motivation theory and information security behaviour. *International Journal of Information Security and Privacy (IJISP)*, *9*(1), 26-46.

Sreenath, S. S. R., Hewitt, B., & Sreenath, S. (2025). Understanding security behaviour among healthcare professionals by comparing results from technology threat avoidance theory and protection motivation theory. *Behaviour & Information Technology*, *44*(2), 181-196. https://doi.org/10.1080/0144929x.2024.2314255

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, *24*(2), 124-133. https://doi.org/10.1016/j.cose.2004.07.001

Sweller, J. (2019). Cognitive load theory and educational technology. *Educational Technology Research and Development*, *68*(1), 1-16. https://doi.org/10.1007/s11423-019-09701-3

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review*, *22*(6), 664-670. https://doi.org/10.2307/2089195

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awareness on information technology professionals' behavior. *Computers & Security*, *79*, 68-79. https://doi.org/10.1016/j.cose.2018.08.007

Trang, S., & Brendel, B. (2019). A meta-analysis of deterrence theory in information security policy compliance research. *Information Systems Frontiers*, *21*(6), 1265-1284. https://doi.org/10.1007/s10796-019-09956-4

Van Maanen, J. (1979). The fact of fiction in organizational ethnography. *Administrative Science Quarterly*, *24*(4), 539-550. https://doi.org/10.2307/2392360

Van Slyke, C., & Belanger, F. (2020). Explaining the interactions of humans and artifacts in insider security behaviors: The mangle of practice perspective. *Computers & Security*, *99*. https://doi.org/10.1016/j.cose.2020.102064

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating is security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3-4), 190-198. https://doi.org/10.1016/j.im.2012.04.002

Vedadi, A., Warkentin, M., Straub, D. W., & Shropshire, J. (2024). Fostering information security compliance as organizational citizenship behavior. *Information & Management*, *61*(5). https://doi.org/10.1016/j.im.2024.103968

Vrhovec, S., & Mihelič, A. (2021). Redefining threat appraisals of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation. *Computers & Security*, *106*. https://doi.org/10.1016/j.cose.2021.102309

Warkentin, M., Walden, E., Johnston, A. C., & Straub, D. W. (2016). Neural correlates of protection motivation for secure it behaviors: An fmri examination [Article]. *Journal of the Association for Information Systems*, *17*(3), 194-215. https://uplib.idm.oclc.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=115434112&site=ehost-live&scope=site

Workman, M. (2007). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, *59*(4), 662-674. https://doi.org/10.1002/asi.20779

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

World Economic Forum. (2025). *Global cybersecurity outlook 2025 - insight report january 2025*. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

Yang, C.-G., & Lee, H.-J. (2016). A study on the antecedents of healthcare information protection intention. *Information Systems Frontiers*, *18*(2), 253-263. https://doi.org/10.1007/s10796-015-9594-x

Zhen, J., Xie, Z., Dong, K., & Chen, L. (2021). Impact of negative emotions on violations of information security policy and possible mitigations. *Behaviour & Information Technology*, *41*(11), 2342-2354. https://doi.org/10.1080/0144929x.2021.1921029

Zscaler. (2024). *Zscaler threatlabz 2024 phishing report*. https://zerotrust.cio.com/wp-content/uploads/sites/64/2024/09/threatlabz-phishing-report-2024.pdf

7. Appendix A

Table 3 – Literature analysis and synthesis matrix

Authors Name and Year of Publication	**Journal**	**Level of Analysis**	**Theories/Models/Constructs**	**Findings**	**Synthesis**
Workman et al. (2008)	Computers in Human Behavior	Micro/Meso -Users of a large technology-oriented company across U.S	• Threat Control Model • Social Cognitive Theory	Highlighted the problem of the "Knowing-Doing" Gap. User claim to prevent a threat, but the likelihood of the event may nullify the action.	Extends the PMT to include internal and external locus of control. Behaviour is explained by a user's control over the event.
Workman et al. (2009)	Behaviour and Information Technology	Micro/Meso - Users of a large technology-oriented company across U.S	• Threat Control Model • Procedural Justice	Link between individual and organisational factors through organisational procedural justice. Users are more inclined to act when they perceive organisational fairness.	Extended PMT to study the link between individual and organisational to incorporate procedural justice.

Lee and Larsen (2009)	European Journal of Information Systems	Micro – SMB Executives in US	• Vendor Support • Firm Size • IT Budget	Adoption of Anti-Malware software in organisations	Extended PMT to examine the behaviour of executives to adopt anti-malware software.
Herath and Rao (2009)	European Journal of Information Systems	Micro/Meso/Macro – Users from diverse roles from organisations across the U.S	• Theory of Planned Behaviour • Deterrence Theory • Organisational behaviour	Resource Availability, Attitude and Social Influence influences behaviour. Organisational Commitment positively behaviour	In the sample it is the first paper to use Theory of Planned Behaviour and Deterrence Theory
Vance et al. (2012)	Information and Management	Micro/Meso – Individual Users of a single municipal organisation were surveyed.	• Habit Theory	Habit is a strong predictor of compliance to organisational policies.	First to introduce Habit into PMT studies
Ifinedo (2012)	Computers and Security	Macro/Meso/Micro – users from cross Industries surveyed from Canada	• Theory of Planned Behaviour	Highlights the benefits of fusing the two theories. User behaviour is based on social, individual, threat and coping factors	Introduced social factors to the discourse and argues for the fusion of various theories in the field

Yoon and Kim (2013)	Information Technology and People	Macro/Meso/Micro – users from cross Industries surveyed in Korea	• Theory of Reasoned Action • Moral Obligation	Organisational norms directly impact user behaviour, and moral obligation also has a role.	Introduces the ethics component within an organisational setting.
Siponen et al. (2014)	Information and Management	Macro/Meso/Micro – users from four corporations across Finland	• Theory of Reasoned Action • Cognitive Evaluation Theory	Normative beliefs and Attitude have a positive impact on users' behaviour	Introduces Attitude, Normative Beliefs and Rewards.
Safa et al. (2015)	Computers and Security	Macro/Meso/Micro – Information Security Experts and Information Technology Professional in Malaysian organisations	• Theory of Planned Behaviour • Information Security Awareness • Organisational Policies • Experience • Attitude • Subjective Norms	Demonstrated that information conscientious care is formed from awareness, policy and procedures, and experience and involvement.	Introduces user experience, policy awareness and procedures as factors that influences Attitude, Social Norms and Self-Efficacy
Posey et al. (2015)	Journal of Management Information Systems	Macro/Meso/Micro – users from various industries across the U.S	• SETA Programs • Organisational Commitment	Organisational SETA efforts improve users	Security Education and Training Awareness was included in this

				threat and coping appraisals on PMT	paper to augment PMT
Johnston et al. (2015)	MIS Quarterly	Macro/Meso/Micro – users from multiple sub organisational offices	• Deterrence Theory • Rhetorical Frameworks	Applicability of informal and formal in deterrence rhetoric	Extended the PMT with a fear appeal rhetorical to enhance behaviour
Jansen et al. (2016)	Behaviour and Information Technology	Micro- Dutch Entrepreneurs	• Attitude • Locus of Control	Adoption of online protective behaviours	Extends PMT to explore online protective behaviours
Chou and Chou (2016)	Computers in Human Behavior	Macro/Meso/Micro – Primary and Secondary school teachers in Taiwan	• Social Norms	Social norms did not explain problematic user behaviour	Extended the PMT to an educational context and included Social Norms
Johnston et al. (2016)	European Journal of Information Systems	Macro- Online Survey gathering data from user who are employed and work in an environment where they must follow security policies	• Big Five Personality Traits • Sanction Severity • Sanction Certainty	Dispositional and Situational factors influence behaviour to comply	Introduced personality meta-traits as a factor into information security

Yang and Lee (2016)	Information Systems Frontiers	Meso – health Information Systems Users in a University Hospital in Korea	• Deterrence Theory • Security Systems Satisfaction/Self Defence Intension • Induction Control Intension	Awareness of consequences of threats improves security behaviour	Extension to the health industry with self-defence and control intension
Hovav and Putri (2016)	Pervasive and Mobile Computing	Macro/Meso/Micro – Mobile workforce in cross industrial organisations across UK, US and UAE	• Top-management participation • Attitude • Subjective norms • Perceived severity of sanctions • Perceived certainty of sanctions	National Cyber Policies and BYOD affect users security behaviour	Moves the focus to a national policy level and perspective of the mobile work
Burns et al. (2017)	Computers in Human Behaviour	Macro/Meso – Users from public and private organisations across the US	• Psychological Capital • Positive Psychology • Hope • Resilience • Optimism	Positive psychological factors improve users coping appraisal	Extends PMT with hope, resilience and optimism as constructs to consider improving security behaviour

Menard et al. (2018)	Computers and Security	Macro– Users from China and U.S asked to work-based scenario survey	• Psychological ownership • Collectivism • Individualism	Psychological ownership improves users' propensity to behave accordingly	Extended to the study the role of culture in security through collectivism and individualism, adding to cross cultural research
Torten et al. (2018)	Computers and Security	Macro/Meso/Micro – IT Professionals from various organisations across the U.S	• Threat Awareness • Countermeasure Awareness • Desktop Security Behaviour	IT Professional are more aware of security threats and awareness plays a crucial role in security	Studied IT professionals and the effect of awareness on their PMT
Blythe and Coventry (2018)	Computers in Human Behavior	Macro/Meso/Micro – Online, employed and computer users	• Experience • Psychological Ownership • Organisational Citizenship • Security Responsibility	Extending PMT with these constructs can explain users behaviours better	Extended the PMT to predict anti-malware behaviour and emphasis the need for extending PMT.
Hanus et al. (2018)	Data Base for Advances in Information Systems	Micro/Meso – Users of a municipality	• Technology Threat Avoidance Theory	Introduces and defines the concept of Security Awareness, and Training will be	Uses PMT as a basis with TTAT and promotes the

			• Theory of Reasoned Action • Theory of Planned Behaviour	better if Interest in Information Security is shown	idea of Security Awareness
Chen et al. (2018)	Journal of Computer Information Systems	Micro/Meso – Employees of a mid-sized University in the U.S	• Deterrence Theory • Rational Choice Theory	Emphasises the importance of SETA programs	Attempt at a unifying model using PMT as one of the models
Moody et al. (2018)	MIS Quarterly	Macro/Meso – workers selected from a professional database at a university in Finland	• Neutralisation theory • Health belief model • Theory of reasoned action • Theory of interpersonal behaviour • Deterrence theory and rational choice • Theory of planned behaviour • Theory of self-regulation	Unifying Information Security theories into UMISPC. Role value, Moral Beliefs, Social factor, Deterrent and Rewards were shown to be constructs to use in studying security. Advocates for habits to be studied.	Attempted to unify prominent theories into a single model

			• Extended parallel processing model • Control balance theory		
Hina et al. (2019)	Computers and Security	Macro/Micro/Meso – employees of High Educational Institutions in Malaysia	• Theory of planned behaviour	Emphasises the importance of Information Security Policies and SETA programs. Includes personal negative experiences as a source of awareness.	Extended PMT to HEI context
Rajab and Eydgahi (2019)	Computers and Security	Meso/Micro – Staff and Faculty of Higher Education institution	• Theory of Planned Behaviour • Deterrence Theory • Organisational Theory	No evidence for Theory of Planned Bahaviour, Deterrence Theory and Organisational Theory in Higher Education	Emphasis the PMT is the most relevant in information security policy compliance in Higher Educations.
Li et al. (2019)	International Journal of Information Management	Macro/Meso/Micro – Employees from various organisation in U.S	• Cues to action • Peer Behaviour	Users observe their peer behaviour for cues to action, cues to action positively	Extends PMT to include cues to action and how users are

				influence user behaviour	influenced by others
Mutchler and Warkentin (2020)	Journal of Database Management	Meso/Micro – Working students, faculty and professionals of a large university in the U.S	• Vicarious Threat Experience • Vicarious Response Experience	Proposes the role of vicarious experience within security behaviour, and justifies for the inclusion of experience in PMT	Extends PMT with the role of vicarious experience
Khan and AlShare (2019)	Journal of Organisational Computing and Electronic Commerce	Meso – employees of mid-western university in U.S	• Individual's traits • Information security policy • Work environment	Violators and Non-violators of security policies differ in these three factors	2 level of study, including Individual, Organisational
Aurigemma and Mattson (2019)	Journal of the Association for Information Systems	Meso – employees from the Department of Defence in the U.S	• Theory of Planned Behaviour • Deterrence Theory • Rational Choice Theory	No single or pseudo universal model applies to any single context only	Studied PMT together with other theories to study its applicability in specific contexts – USB Flash use, Phishing and Tailgating
Hooper and Blunt (2020)	Behaviour and Information Technology	Macro/Meso – IT employees of government and	• Cues to Action • Social Norms	Differentiates between normal and ICT	Applies and extends PMT to

		other organisations across New Zealand	• Detection • Sanctions	employees. Cues to action, perceived impact and self-efficacy will impact IT employee behaviour	focus on IT employees
Ameen, Tarhini, Shah, et al. (2020)	Computers in Human Behaviour	Macro – Gen Mobile employee across Uk, US, UAE	• National Factors • Organisational Factors • Technological Factor • Personal Factors	Explains employees behaviour influenced by national cyber security policies	Extend PMT to an international context
Schuetz et al. (2020)	Journal of Management Information Systems	Meso – Organisational users from a large US university	• Construal Level Theory	Proposes degree of abstraction and that concrete messages are more effective	Extended PMT to understand fear appeal deign
Ogbanufe (2021)	Computers and Security	Macro/Meso – Various organisations from within the U.S	• Awareness • Threat • Organisational support • Role Identity	Organisational culture allows one to understand their role that support security behaviour	Extends the PMT threat appraisals with awareness and organisational support to influence role identity
Vrhovec and Mihelič (2021)	Computers and Security	Meso – University academics at six	• Organisational Level Severity and Vulnerability.	Threat and Vulnerability perception varies at the levels as the	Differentiates between Individual and

		universities in Slovenia	• Individual Level Severity and Vulnerability	role of fear may be interpreted differently	Organisational level
McLeod and Dolezel (2022)	Computers and Security	Meso – Setting states ISP compliance it is inferred it is in an organisational context, but not explicitly mentioned in method	• Technology Threat Avoidance Theory • Capitulation Theory	If threats were to happen there is nothing users will do to stop it	Extends PMT with capitulation theory
Ameen, Tarhini, Hussain Shah, et al. (2020)	Computers in Human Behavior	Macro/Meso – Employees from Multi-National organitions in UAE and U.S	• Deterrence Theory • Culture Theory	Gender influence on security behaviour.	Extended PMT to study the influence of gender on behaviour
Jaeger and Eckhardt (2021)	Information Systems Journal	Macro/Meso – employees from organisations in Western Europe	• Perceptual Cycle Models • Awareness • Individual and System Level construct	Awareness, situational information security awareness	Extended PMT to situational awareness
Chen et al. (2021)	Information Systems Research	Macro – Employees from organisations	• Extended Parallel Processing Model	Higher threat is associated with higher fear	EPPM was extended with PMT constructs

		anywhere in the U.S	• Adaptive and Maladaptive coping		
Shahbaznezhad et al. (2021)	Journal of Computer Information Systems	Meso – Two organisations in New Zealand where employees surveyed	• Theory of Planned Behaviour • SETA Theory • Deterrence Theory • Technological Factor	Individual, organisational and technological factors leading to behaviour to click on phishing emails	PMT was extended with other theories to explore the socio-technical perspective in phishing emails
Schuetz et al. (2021)	Journal of the Association for Information Systems	Not explicitly specified but they allude to the impact of their study of organisation and highlights organisational security in their Keywords	• Construal-Level Theory • Fear Appeal Design	Temporal distance and argument nature. How to avert and deal with a threat and it is important to do so	Extended PMT with the construal theory to understand security messaging and its effectiveness to users
Aigbefo et al. (2022)	Behaviour and Information Technology	Macro – working SME population from U.S, UK and Australia	• Habit theory • Theory of Planned Behaviour • Personality Traits	Hardiness, positive habits are good for security behaviour	Extended previous studies to include personality traits such as hardiness

Sharma and Aparicio (2022)	Computers and Security	Meso/Macro – IT employees from U.S	• Organisational and Institutional theory	Interaction between cultural factors has an impact on security behaviour	Extended PMT with espoused organisation culture and team culture
Li et al. (2022)	Computers in Human Behaviour Reports	Meso/Macro – Employees from various organisations across the east coast of the U.S	• Organisational Information Security Effort • Employee Security Effort • Demographic Information	Demographics, Awareness and organisational investment influences behaviour	Extended PMT with Awareness, demographics and Organisational efforts
Ma (2022)	Information Processing and Management	Meso/Macro – employees with IT industry	• Theory of Planned Behaviour • Job Satisfaction • Organisational Commitment	The constructs have an influence on security behaviour	Extended PMT with Theory of Planned Behaviour, Job Satisfaction and Organisational Commitment
Wong et al. (2022)	International Journal of Information Management	Meso – SME workforce	• SETA programs • Awareness	Employee education in security is important	Extended PMT with SETA

Johnston et al. (2023)	Computers and Security	Meso – Working professionals in the U.S	• Rhetorical Framework • Extended Parallel Processing Model	Importance of Rhetorically applicability of fear messaging	Extended PMT with Rhetoric Theory and EPPM
Ogbanufe et al. (2023)	Computers and Security	Meso – Employees working from home in the U.S	• Stewardship Theory • Psychological ownership	PMT was more likely to explain behaviour of users working from home than Stewardship theory	Extended PMT with Stewardship theory and Working from home
Bekkers et al. (2023)	Computers and Security	Meso – Entrepreneurs from SME's in the Netherlands	• Social Norms • SETA Programs	Outsourcing IT will decrease sensitivity to security threats	Extended PMT with Social norms and SETA awareness
(Ogbanufe & Ge, 2023)	Computers and Security	Meso/Macro – employees from various industries across U.S	• Stewardship Theory • Organisational Theory • Demographics	Internalisation, sense making process, role performance and security setting is important	Extending PMT to Information security setting and demographics
Chen et al. (2023)	Australian Journal of Public Administration	Meso – Civil servants of Chinese government	• Organisational Theory • Organisational Culture	Organisational culture influence security awareness	Extended PMT with Organisational theories in the Chinese context

Aggarwal and Srivastava (2024)	Computers and Security	Meso/Macro – employees within the financial banking and non-banking sector within India	• Transactional Model of Stress and Coping • Eustress	Highlights importance of fear, fear appeals and eustress in influencing behaviour	Extends PMT to include stress and positive stress
Green et al. (2024)	Computers and Security	Meso/Macro – IS professionals who had reported vulnerabilities to organisations in U.S	• Vulnerability Discovery and Disclosure Model	Cooperative vs Antagonistic approaches	Extends PMT to study Researcher and Organisational threat severity and vulnerability
Kim et al. (2024)	Current Psychology	Meso/Macro – employees from various organisations in South Korea	• Job Demand Resources Theory • Social Identity Theories	Work overload influences behaviour	Extend PMT with job stress and organisational identification
Nastjuk et al. (2024)	European Journal of Information Systems	Meso/Macro – Employee training from four German organisations	• SETA Programs	Differentiate between training output and sustained training output	Extended PMT with SETA
Mukhopadhyay and Jain (2024)	International Journal of Information Management	Macro/Macro – Organisations from critical and non-critical sectors in	• Organisational Structure • Technological Factors	Ensuring technical factors are considered	Extend PMT into Technological Factors

		US, Australia, Canada and Japan	• Information Security Governance		
Tran, Nguyen, Nguyen, et al. (2024)	Journal of Asia Business Studies	Meso/Macro – employees from various organisations in Vietnam	• Cultivation Theory	Government Social Media as a platform to enhance security	Extends PMT with cultivation Theory
Tran, Nguyen, Vrontis, et al. (2024)	Journal of Asia Business Studies	Meso/Macro – government employees in Vietnam	• Cultivation Theory	Awareness and not policy itself has an influence on behaviour	Extends PMT with cultivation Theory
Sreenath et al. (2025)	Behaviour and Information Technology	Macro – health care professionals in the US	• Technology Threat Avoidance Theory	Argue that TTAT is a better model than PMT	Compares PMT to TTAT and finds TTAT more applicable in healthcare setting
Alrawhani et al. (2025)	International Journal of Human-Computer Interaction	Meso/Macro – Banking employees in Yemen	• Organisational Culture	Finds PMT appropriate to study behaviour	Extends PMT to understand Information Security Culture
Ganye and Smith (2025)	Internet Research	Meso – general users of information system	• Cognitive Load theory • Rational Choice theory	Cognitive Load has an influence on behaviour	Extends PMT with Cognitive Load and Rational choice Theories.

		of an organisation in the EU			

7.1 Synthesis – References

Aggarwal, A., & Srivastava, S. K. (2024). Exploring eustress and fear: A new perspective on protection motivation in information security policy compliance within the financial sector. *Computers & Security*, *142*. https://doi.org/10.1016/j.cose.2024.103857

Aigbefo, Q. A., Blount, Y., & Marrone, M. (2022). The influence of hardiness and habit on security behaviour intention. *Behaviour & Information Technology*, *41*(6), 1151-1170. https://doi.org/10.1080/0144929x.2020.1856928

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. https://doi.org/10.1080/10447318.2025.2464900

Ameen, N., Tarhini, A., Hussain Shah, M., & Madichie, N. O. (2020). Employees' behavioural intention to smartphone security: A gender-based, cross-national study. *Computers in Human Behavior*, *104*. https://doi.org/10.1016/j.chb.2019.106184

Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., & Choudrie, J. (2020). Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the gen-mobile workforce. *Computers in Human Behavior*, *114*, Article 106531. https://doi.org/10.1016/j.chb.2020.106531

Aurigemma, S., & Mattson, T. (2019). Generally speaking, context matters: Making the case for a change from universal to particular isp research. *Journal of the Association for Information Systems*, 1700-1742. https://doi.org/10.17705/1jais.00583

Bekkers, L., van 't Hoff-de Goede, S., Misana-ter Huurne, E., van Houten, Y., Spithoven, R., & Leukfeldt, E. R. (2023). Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model. *Computers & Security*, *127*. https://doi.org/10.1016/j.cose.2023.103099

Blythe, J. M., & Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior*, *87*, 87-97. https://doi.org/10.1016/j.chb.2018.05.023

Burns, A. J., Posey, C., Roberts, T. L., & Benjamin Lowry, P. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, *68*, 190-209. https://doi.org/10.1016/j.chb.2016.11.018

Chen, L., Zhen, J., Dong, K., & Xie, Z. (2023). Organisational culture and information security awareness of chinese grassroots civil servants: A mediated moderation model. *Australian Journal of Public Administration*, *83*(3), 372-393. https://doi.org/10.1111/1467-8500.12596

Chen, X., Chen, L., & Wu, D. (2018). Factors that influence employees' security policy compliance: An awareness-motivation-capability perspective. *Journal of Computer Information Systems*, *58*(4), 312-324. https://doi.org/10.1080/08874417.2016.1258679

Chen, Y., Galletta, D. F., Lowry, P. B., Luo, X., Moody, G. D., & Willison, R. (2021). Understanding inconsistent employee compliance with information security policies through the lens of the extended parallel process model. *Information Systems Research*, *32*(3), 1043-1065. https://doi.org/10.1287/isre.2021.1014

Chou, H.-L., & Chou, C. (2016). An analysis of multiple factors relating to teachers' problematic information security behavior. *Computers in Human Behavior*, *65*, 334-345. https://doi.org/10.1016/j.chb.2016.08.034

Ganye, D., & Smith, K. (2025). Examining the effects of cognitive load on information systems security policy compliance. *Internet Research*, *35*(1), 380-418. https://doi.org/10.1108/intr-04-2023-0329

Green, A. W., Oliver, D., & Woszczynski, A. B. (2024). To report or not to report? Extending protection motivation theory to vulnerability discovery and disclosure. *Computers & Security*, *142*, Article 103880. https://doi.org/10.1016/j.cose.2024.103880

Hanus, B., Windsor, J. C., & Wu, Y. (2018). Definition and multidimensionality of security awareness: Close encounters of the second order. *SIGMIS Database*, *49*(SI), 103–133. https://doi.org/10.1145/3210530.3210538

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

Hina, S., Panneer Selvam, D. D. D., & Lowry, P. B. (2019). Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computers & Security*, *87*. https://doi.org/10.1016/j.cose.2019.101594

Hooper, V., & Blunt, C. (2020). Factors influencing the information security behaviour of it employees. *Behaviour & Information Technology*, *39*(8), 862-874. https://doi.org/10.1080/0144929x.2019.1623322

Hovav, A., & Putri, F. F. (2016). This is my device! Why should i follow your rules? Employees' compliance with byod security policy. *Pervasive and Mobile Computing*, *32*, 35-49. https://doi.org/10.1016/j.pmcj.2016.06.007

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95. https://doi.org/10.1016/j.cose.2011.10.007

Jaeger, L., & Eckhardt, A. (2021). Eyes wide open: The role of situational information security awareness for security-related behaviour. *Information Systems Journal*, *31*(3), 429-472. https://doi.org/10.1111/isj.12317

Jansen, J., Veenstra, S., Zuurveen, R., & Stol, W. (2016). Guarding against online threats: Why entrepreneurs take protective measures. *Behaviour & Information Technology*, *35*(5), 368-379. https://doi.org/10.1080/0144929x.2016.1160287

Johnston, A., Di Gangi, P. M., Belanger, F., Crossler, R. E., Siponen, M., Warkentin, M., & Singh, T. (2023). Seeking rhetorical validity in fear appeal research: An application of rhetorical theory. *Computers & Security*, *125*, Article 103020. https://doi.org/10.1016/j.cose.2022.103020

Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and situational factors: Influences on information security policy violations. *European Journal of Information Systems*, *25*(3), 231-251. https://doi.org/10.1057/ejis.2015.15

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework. *MIS Quarterly*, *39*(1), 113-134.

Khan, H. U., & AlShare, K. A. (2019). Violators versus non-violators of information security measures in organizations—a study of distinguishing factors. *Journal of Organizational Computing and Electronic Commerce*, *29*(1), 4-23. https://doi.org/10.1080/10919392.2019.1552743

Kim, B.-J., Kim, M.-J., & Lee, J. (2024). Examining the impact of work overload on cybersecurity behavior: Highlighting self-efficacy in the realm of artificial intelligence. *Current Psychology*, *43*(19), 17146-17162. https://doi.org/10.1007/s12144-024-05692-4

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of smb executives' decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(2), 177-187. https://doi.org/10.1057/ejis.2009.11

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13-24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

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

Ma, X. (2022). Is professionals' information security behaviors in chinese it organizations for information security protection. *Information Processing & Management*, *59*(1). https://doi.org/10.1016/j.ipm.2021.102744

McLeod, A., & Dolezel, D. (2022). Information security policy non-compliance: Can capitulation theory explain user behaviors? *Computers & Security*, *112*. https://doi.org/10.1016/j.cose.2021.102526

Menard, P., Warkentin, M., & Lowry, P. B. (2018). The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. *Computers & Security*, *75*, 147-166. https://doi.org/10.1016/j.cose.2018.01.020

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*(1), 285-311. https://doi.org/10.25300/misq/2018/13853

Mukhopadhyay, A., & Jain, S. (2024). A framework for cyber-risk insurance against ransomware: A mixed-method approach. *International Journal of Information Management*, *74*. https://doi.org/10.1016/j.ijinfomgt.2023.102724

Mutchler, L. A., & Warkentin, M. (2020). Experience matters: The role of vicarious experience in secure actions. *Journal of Database Management*, *31*(2), 1-20. https://doi.org/10.4018/jdm.2020040101

Nastjuk, I., Rampold, F., Trang, S., & Benitez, J. (2024). A field experiment on isp training designs for enhancing employee information security compliance [;

Early Access]. *European Journal of Information Systems*. https://doi.org/10.1080/0960085x.2024.2359460

Ogbanufe, O. (2021). Enhancing end-user roles in information security: Exploring the setting, situation, and identity. *Computers & Security*, *108*. https://doi.org/10.1016/j.cose.2021.102340

Ogbanufe, O., Crossler, R. E., & Biros, D. (2023). The valued coexistence of protection motivation and stewardship in information security behaviors. *Computers & Security*, *124*. https://doi.org/10.1016/j.cose.2022.102960

Ogbanufe, O., & Ge, L. (2023). A comparative evaluation of behavioral security motives: Protection, intrinsic, and identity motivations. *Computers & Security*, *128*. https://doi.org/10.1016/j.cose.2023.103136

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), 179-214. https://doi.org/10.1080/07421222.2015.1138374

Rajab, M., & Eydgahi, A. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers & Security*, *80*, 211-223. https://doi.org/10.1016/j.cose.2018.09.016

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65-78. https://doi.org/10.1016/j.cose.2015.05.012

Schuetz, S. W., Benjamin Lowry, P., Pienta, D. A., & Bennett Thatcher, J. (2020). The effectiveness of abstract versus concrete fear appeals in information security. *Journal of Management Information Systems*, *37*(3), 723-757. https://doi.org/10.1080/07421222.2020.1790187

Schuetz, S. W., Lowry, P. B., Pienta, D. A., & Thatcher, J. B. (2021). Improving the design of information security messages by leveraging the effects of temporal distance and argument nature. *Journal of the Association for Information Systems*, *22*(5), 1376-1428. https://doi.org/10.17705/1jais.00697

Shahbaznezhad, H., Kolini, F., & Rashidirad, M. (2021). Employees' behavior in phishing attacks: What individual, organizational, and technological factors matter? *Journal of Computer Information Systems*, *61*(6), 539-550. https://doi.org/10.1080/08874417.2020.1812134

Sharma, S., & Aparicio, E. (2022). Organizational and team culture as antecedents of protection motivation among it employees. *Computers & Security*, *120*, Article 102774. https://doi.org/10.1016/j.cose.2022.102774

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, *51*(2), 217-224. https://doi.org/10.1016/j.im.2013.08.006

Sreenath, S. S. R., Hewitt, B., & Sreenath, S. (2025). Understanding security behaviour among healthcare professionals by comparing results from technology threat avoidance theory and protection motivation theory. *Behaviour & Information Technology*, *44*(2), 181-196. https://doi.org/10.1080/0144929x.2024.2314255

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awareness on information technology professionals' behavior. *Computers & Security*, *79*, 68-79. https://doi.org/10.1016/j.cose.2018.08.007

Tran, D. V., Nguyen, P. V., Nguyen, A. T. C., Vrontis, D., & Dinh, P. U. (2024). Exploring the influence of government social media on cybersecurity compliance: Employee attitudes, motivation and behaviors. *Journal of Asia Business Studies*, *18*(1), 204-223. https://doi.org/10.1108/JABS-09-2023-0343

Tran, D. V., Nguyen, P. V., Vrontis, D., Nguyen, S. T. N., & Dinh, P. U. (2024). Unraveling influential factors shaping employee cybersecurity behaviors: An empirical investigation of public servants in vietnam. *Journal of Asia Business Studies*, *18*(6), 1445-1464. https://doi.org/10.1108/jabs-01-2024-0058

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating is security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3-4), 190-198. https://doi.org/10.1016/j.im.2012.04.002

Vrhovec, S., & Mihelič, A. (2021). Redefining threat appraisals of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation. *Computers & Security*, *106*. https://doi.org/10.1016/j.cose.2021.102309

Wong, L.-W., Lee, V.-H., Tan, G. W.-H., Ooi, K.-B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*, *66*, Article 102520. https://doi.org/10.1016/j.ijinfomgt.2022.102520

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

Workman, M., Bommer, W. H., & Straub, D. (2009). The amplification effects of procedural justice on a threat control model of information systems security behaviours. *Behaviour & Information Technology*, *28*(6), 563-575. https://doi.org/10.1080/01449290802556021

Yang, C.-G., & Lee, H.-J. (2016). A study on the antecedents of healthcare information protection intention. *Information Systems Frontiers*, *18*(2), 253-263. https://doi.org/10.1007/s10796-015-9594-x

Yoon, C., & Kim, H. (2013). Understanding computer security behavioral intention in the workplace an empirical study of korean firms. *Information Technology & People*, *26*(4), 401-419. https://doi.org/10.1108/itp-12-2012-0147

8. Appendix B – Grouping of First and Second-order Constructs

Table 4 - First and Second order constructs

Second Order Theory, Theme, Model or Framework	**First-Order Contructs**
Theory of Planned Behaviour	• Attitude • Perceived behavioural control (Self-Efficacy) • Resource availability • Subjective norms
Deterrence Theory	• Certainty of Detection • Certainty of Sanctions • Formal Sanctions • Informal Sanctions • Severity of Sanctions
Organisational Theory	• Ethical leadership • Organizational characteristics • Organizational culture • Top management support
Organisational Culture	• Adaptibility • Basic Assumptions • Consistency • Involvement • ISP Compliance • Material Layer • Mission • Perceived mutualism justice • Rule Orientation • Supportive Values
Big Five Personality Model	• Agreeableness • Conscientiousness • Extraversion • Neuroticism • Openess to Expirience
Cognitive Evaluation Theory	• Autonomy • Intrinsic Motivation • Normative Beliefs • Rewards
Cognitive Load Theory	• Extraneous cognative load • Germane cognitive loads • Intrinsic cognative load
Construal-Level Theory	• Distal Psychological distance • Generic Features

	• Proximate Psychological distance • Psychological distance • Specific Features
Capitulation Theory	• Committment and Effort • Disengagement • Evaluation • Hopelessness • Lack of Autonomy • Lack of Choice
Control Balance Theory	• Constraints • Control Balance • Situational Provocation • Violation Motivation
Cultivation Theory	• Mainstreaming • Perception of Reality • Resonance
Culture Theory	• Culture:Individualim-vs-Collectivism • Culture:Power-Distance • Culture:RoleofGender • Culture:Uncertainty-Avoidance
Expectancy-value Theory	• Perceived importance • Personal responsibility • Responsibility • Security habits • Social norms:descriptive norms and subjective norms
Extended Parralel Process Model	• Adaptive Coping • Defensive Motivation • Emotional Coping • Emotional Focused • External Motivated • Fear Appeal • Individual Level Severity • Individual Level Vulnerability • Internal Motivated • Maladaptive Coping • Organisaional Level Vulnerability • Organisational Level Severity • Problem Focused • Protection Motivation • Response-Efficacy • Self-Efficacy • Severity

	• Susceptibility
Habit Theory	• Automatic Behaviour • Cues • Habit Theory: Routine Behaviour • Heuristics • Past Expirience • Perceived realism • Unconscienscious Behaviour
Hardiness Personality Trait	• Hardiness:Challenge • Hardiness:Commitment • Hardiness:Contol
Health Belief Model	• Cues to action
Job-Demand Resources Theory	• Job stress • Workload
Neuropharmacological Trait Theory	• Derived Perceptions - Sanctions perceptions • Dispositional - Personality Traits • Situational Factors:Sanctions and Training Rhetoric
Organisation Characteristics	• Confidentiality of Information • Reliance on Information Systems
Organisational Culture	• Adaptibility • Basic Assumptions • Consistency • Involvement • Material Layer • Mission • Organizational culture include involvement, consistency, adaptability, and • Perceived mutualism justice • Supportive Values
Organisational Environment	• Cues to action • Peer behavior • Prior information security experience
Organisational and Institutional Theory	• Ethical leadership • Organisational characteristics • Organisational culture • Top management support
Perceptual Cycle Models (PCM) of situation Awareness	• Agreeableness • Contextual Relevance • Experience • Misplaced Salience • Security Warning
Psychological Capital	• Hope • Optimism

	• Resilience
Psychological ownership	• Collectivism • Psychological ownership: Individual
Rational Choice Theory	• message acceptance • Message rejection • Perceived Benefits of Compliance • Perceived cost of compliance • Perceived Cost of non-compliance
Reaction Theory	• Free behaviour
Rhetorical Framework	• Threat to Human Asset: Enhanced Rhetoric • Threat to Information Asset: Conventional Rhetoric • Validity and Contextualisation
Self-Determination Theory	• Autonomy • Competence • Relatedness
Social Cognitive Theory	• Procedural justice
Social Identity theory (Organisational Identification)	• Extra-Role Security Behaviour • In-Role Security Behaviour • Indentity • Information Security Role Identity
Stewardship Theory	• Autonomy • Collectivism • Organisational Commitment • Organisational Support • Psycological Ownership
Technology Threat Avoidance Theory	• Avoidability • Perceived Threat • Safeguard Cost • Safeguard Effectiveness
Theory of Interpersonal Behaviour	• Affect • Attitude • Costs • Facilitating Conditions • Habit • Rewards • Self-Concept • Social Influence • Subjective Norms
Theory of Motivational Stress Coping	• Eustress • Fear
Theory of Neutralisation	• Justifying Transgression
Theory of Reasoned Action	• Attitude

	• Moral obligation • Organizational norms
Theory of Self-Regulation	• Attitude • Desire • Subjective Norms
Threat Control Model	• Subjective and Objective Omissive behavior
Vulnerability Discovery and Disclosure Model	• Observational Learning • Personality Variables • Prior expirience • Verbal Persuation
Organisational Justice Theory	• Procedural Justice • Distributive Justice • Interactive Justice
Fear-Appeal Design	• Abstract • Concrete • Frequency of Communication • Messages with How Arguments • Messages with Why Arguments • Organisational Audience • Personal Audience • Temporal Distance
Individual Traits	• Privacy • Trust
Locus of Control	• External Locus of Control • Internal Locus of Control
SETA programs	• SETA Frequency • SETA Training • Threat Awareness • Training Design
Team culture	• Ethical Leardership • ISP Compliance • Rule Orientation
Technological Factors	• Digital Intensity • Investment • Technology Use
Transactional Model of Stress and Coping	• Eustress • Fear
No Second Order themes	• Vicarious Expirience • Awareness