Managing Risks and Perceptions in Everyday Organisational Cybersecurity

Sunitha Prabhu
School of Management and Marketing
Curtin University
Perth, Australia
Email: sunitha.prabhu@postgrad.curtin.edu

Abstract

Employee compliance is crucial for effective cybersecurity, yet the underlying psychological drivers of risky behaviours remain complex. Deliberate cybersecurity risks can arise through active behaviours (actions) or passive behaviours (inaction). Despite growing conceptual recognition of this distinction, empirical evidence remains limited. This study examines how threat perception and neutralisation differentially shape cybersecurity intentions across these two risk domains. Survey data from 490 UK employees, covering four common cybersecurity behaviours were analysed. The findings show that both perceived threat and neutralisation significantly influence intentions, but in different ways. Neutralisation more strongly predicts active risk-taking, whereas perceived threat is a stronger predictor of passive risk-taking. Moreover, passive risk-taking was reported more frequently than active risk-taking, challenging assumptions that employee-driven cybersecurity vulnerabilities primarily stem from overt policy violations. By identifying distinct psychological mechanisms underlying active and passive risk-taking, this study provides practical insights for the design of targeted cybersecurity interventions. Future studies could examine contextual factors that moderate the interplay between threat perception and neutralisation across risk domains.

Keywords Information security, Active risk, Passive risk, Perceived threat, Neutralisation.

1 Introduction

A common misconception in organisations is that extensive security information ensures uniform risk perception and compliance (Chowdhury et al., 2020; Hong et al., 2023). In practice, however, when faced with choices involving both benefits and risks, individuals often favour the easier option (Ajzen, 1985). For example, an employee might bypass a Multi-Factor Authentication (MFA) step if given the option, prioritising time saved (benefit) over enhanced security by MFA. Such actions can lead to inconsistent compliance with security policies, increasing organisational vulnerability to cybersecurity threats (Prabhu et al., 2025). Recent industry reports reinforce this concern, with ProofPoint (2023) noting that insider threats cost businesses upward of $15 million annually and were a top concern for 36% of organisations in 2023, up from 31% in 2022.

To minimise these threats, organisations implement security policies. However, employees may *intentionally* deviate from these policies, introducing risks through two distinct pathways: active risk-taking and passive risk-taking behaviours (Keinan & Bereby-Meyer, 2012). It is crucial to distinguish these from accidental lapses, as they are not intentional (Prabhu & Thompson, 2020). *Active risk-taking* involves intentional actions that violate security protocols,

Received 25 June 2025, accepted 03 Dec 2025 after 1 round of review with Humza Naseer as accepting Senior Editor, Michael Davern and Stuart Black as Editors in Chief

such as downloading unlicensed software or sharing sensitive information on unencrypted public Wi-Fi networks (Keinan & Bereby-Meyer, 2012; Prabhu & Thompson, 2020). In contrast,

passive risk-taking involves intentional inaction, like failing to install security updates. Here, risk stems from *inaction* or *omission* (Arend et al., 2020; Keinan & Bereby-Meyer, 2012; Prabhu & Thompson, 2020). These two behavioural forms reflect distinct cognitive pathways, with varying degrees of threat perception and susceptibility to neutralisation strategies.

Understanding the psychological drivers of risk-taking behaviour, such as motivation and rationalisation, provides insight into how individuals perceive and respond to risks (Hooper & Blunt, 2020; Padayachee, 2024). Central to this is *threat perception*, a motivational factor that shapes protective action when an individual recognises a credible danger (Rogers, 1975). This concept, formalised by frameworks like protection motivation theory (PMT) (Rogers, 1975) and Technology Threat Avoidance Theory (TTAT) (Liang & Xue, 2009), can prompt cautious behaviours, such as verifying information sources, updating software, and avoiding risky actions (Hong et al., 2023; Hooper & Blunt, 2020). However, these protective impulses can be weakened by *neutralisation* – self-justifications that allow deviation from protocols without undue moral discomfort (Sykes & Matza, 1957). Repeated risk-taking can dull the initial sensitivity of threat perception, while neutralisation strategies become more ingrained (Vance et al., 2012; Verplanken & Aarts, 1999). This dual dynamic, i.e., a fading sensitivity to threat and a growing reliance on neutralisation, may lead to a self-reinforcing cycle of risk-taking.

To fully capture the nuances of this self-reinforcing cycle, it is crucial to consider the distinct forms of cybersecurity risk-taking. While the conceptual distinction between these risk-taking domains is gaining recognition, prior empirical studies, though affirming the individual roles of threat perception and neutralisation in security compliance, have yet to explore their differential influence across distinct categories of employee-controlled risk behaviours. Empirical research remains limited regarding whether threat perception and neutralisation exert the same influence across active and passive risk-taking behaviours. For instance, does threat perception deter active risk-taking behaviours more than passive ones? Are passive risks more easily neutralised because they feel less intentional? Might passive risks be more frequent due to less cognitive effort? These questions remain underexplored in the cybersecurity literature and form the foundation of the current study.

To explore this critical gap, this study offers a novel empirical investigation into how threat perception and neutralisation differentially influence employees' cybersecurity intentions across active versus passive risk-taking behaviours. The Research Question (RQ) is:

RQ: *How do threat perceptions and neutralisation shape employees' cybersecurity intentions across active and passive risk-taking behaviours?*

To address the RQ while ensuring generalisability, this study examines four common, employee-controlled behaviours: two active risk behaviours (using USB devices and opening unknown links) and two passive risk behaviours (reusing passwords and failing to secure portable devices). Using a survey design, the proposed hypotheses were tested using Structural Equation Modelling (SEM) and multiple regression with a sample of 490 working adults, extending current knowledge by differentiating between psychological predictors (threat perception and neutralisation) of active versus passive security risk behaviours. Our

findings reveal a nuanced relationship: while both threat perceptions and neutralisation significantly influence security intentions, neutralisation exerts a stronger impact on active risk behaviours. Conversely, threat perception is a more potent predictor of passive risk behaviours, yet passive risk behaviours occur more frequently. This suggests that awareness campaigns alone may be insufficient to curb convenience-driven choices or actions deprioritised due to competing demands.

The remainder of this paper is structured as follows: Section 2 covers the theoretical background, leading to the hypotheses in Section 3. Section 4 details the methodology. Section 5 presents the study's results, followed by Section 6, which discusses the key findings, implications, limitations, and suggests avenues for future research. Finally, Section 7 concludes by highlighting the key contributions.

2 Background

Effective cybersecurity hinges on understanding the underlying psychological mechanisms underpinning behaviour. Although threat perception motivates protective action (Rogers, 1975), its influence can be attenuated by the use of neutralisation strategies. The interaction between these cognitive processes is likely to differ across active or passive forms of risk-taking. Thus, understanding the dynamic between threat perception, neutralisation, and risk type is key to explaining the persistence of cybersecurity vulnerabilities within organisations.

2.1 Active and Passive Risk-Taking Behaviours

Intentional cybersecurity risk-taking manifests through two pathways: active and passive. Active risk-taking involves intentional actions that directly introduce vulnerabilities, reflecting what individuals consciously "*do*". In contrast, passive risk-taking stems from intentional inaction, reflecting what individuals "*do not do*" despite awareness of security policies. This includes "*choosing not to act*" or, in some cases, "*choosing not to act for now*" (Arend et al., 2020; Keinan & Bereby-Meyer, 2012). For instance, an employee may knowingly postpone a critical software update despite awareness of the associated risk. This study focuses exclusively on these intentional forms, distinguishing them from accidental or unintentional lapses.

From a psychological perspective, several tendencies contribute to passive risk-taking. The *default effect*, for instance, describes an individual's tendency to maintain the current state rather than initiate change, even when actions could lead to a better security outcome (Samuelson & Zeckhauser, 1988). An example is when employees do not enable MFA or neglect software updates, adhering to pre-existing insecure states.

Passive risk-taking is typically associated with tendencies such as avoidance, omission bias, default bias, inaction inertia, and procrastination (Keinan & Bereby-Meyer, 2012). *Avoidance* involves deliberately steering away from tasks perceived as unpleasant or effortful (Tykocinski & Pittman, 1998). *Omission bias* downplays harmful inactions as less severe than harmful actions (Baron & Ritov, 2004), while default bias encourages adherence to preset options (Samuelson & Zeckhauser, 1988). *Inaction inertia* describes the decreased likelihood of acting on a later opportunity after missing an earlier one (Tykocinski & Pittman, 1998). *Procrastination,* a motivational delay, involves intending to act but postponing it, often diminishing the perceived urgency of the task (Padayachee, 2015). These behaviours, even if only temporarily delayed, often represent conscious decisions.

A key psychological distinction between active and passive risk-taking lies in perceived

accountability. Individuals are generally held more accountable for harmful actions than for harmful inaction, making passive risk-taking appear less deviant than overt misconduct (Arend et al., 2020; Keinan & Bereby-Meyer, 2012). This perception allows inaction-based vulnerabilities to escape scrutiny despite their potentially serious security implications. Beyond accountability, underlying psychological tendencies also diverge: active risk-taking aligns with impulsivity and sensation-seeking, whereas passive risk-taking reflects avoidance, indecision, and procrastination (Keinan & Bereby-Meyer, 2012). Table 1 concisely summarises these key distinctions.

	Active-risk behaviours	**Passive-risk behaviours**
Cause	Risk arises from actions that introduce threats.	Risk arises from inaction, neglect, or failure to follow security best practices.
Examples	Using USB devices, clicking suspicious links, downloading unverified files, granting excessive privileges.	Reusing passwords, failing to update software, leaving devices unsecured or unattended.
Cognitive involvement	May reflect overconfidence in one's ability to manage outcomes or low perceived risk.	Often involves procrastination, avoidance, or habitual inaction.
Associated motivation	Frequently driven by convenience, curiosity, or perceived urgency.	Often motivated by avoidance or a misplaced trust in system safeguards.
Threat evaluations are	Sometimes bypassed due to perceived urgency.	Often overlooked due to negligence or habitual actions.
Typical neutralisation	Justifications like "*This is necessary*" or "*It won't cause harm*" to reduce the psychological burden of risky actions.	Justifying delay, "*I'll do it later*", reduces the sense of urgency without directly justifying risky actions.

Table 1: Active and Passive Risk-Taking

Both active and passive risk-taking are influenced by perceived threat. In active risk scenarios, threats are often more explicit, prompting deliberate decisions with clearer awareness of potential consequences (Rogers, 1975; Sykes & Matza, 1957). Conversely, passive risk scenarios often involve subtler threat perceptions, where individuals might intend to act eventually, creating a false sense of safety (Arend et al., 2020). Neutralisation also provides a means of justification for both active and passive risk-taking. Active risk-taking may be rationalised with justifications like "*this will benefit us*", while passive risk-taking is often minimised with rationalisations such as "*it's fine for now*". Despite their seemingly subtle nature, passive risks can be equally, if not more, consequential, often creating persistent vulnerabilities that can significantly amplify exposure to serious threats like data breaches, malware infections, and data loss (Prabhu & Dell, 2025b).

While these distinctions are clear, the relative influence of threat perceptions and neutralisation processes on the emergence and persistence of active versus passive risk-taking in cybersecurity settings remains underexplored. Addressing this gap holds potential for valuable insights in designing interventions to mitigate both forms of insider threats.

2.2 Threat Perceptions

Perceived threat, a core construct in cybersecurity compliance, primarily drives behaviour by increasing risk awareness and motivating protective action. It reflects an individual's

evaluation of both the potential threat's severity and personal vulnerability (Rogers, 1975). According to PMT, higher perceived threat, characterised by strong feelings of severity and vulnerability, directly enhances motivation for protective behaviours (Rogers, 1975). PMT outlines two response pathways: adaptive (protective actions taken) and maladaptive (threats are downplayed or ignored) (Rogers, 1983). For adaptive responses, employees must not only perceive their vulnerability but also grasp the consequences of their (in)actions (Becker et al., 1974). However, PMT primarily promotes protective action adoption, aligning more closely with reducing passive risks (e.g., enabling MFA) (Liang & Xue, 2009).

Technology Threat Avoidance Aheory (TTAT) offers a complementary perspective by focusing on the avoidance of risk-taking rather than adopting safeguards, making it particularly relevant to active risk-taking scenarios. TTAT helps explain why individuals might avoid actions like using USB devices or clicking phishing links that could lead to security compromises (Liang & Xue, 2009). While both theories emphasise perceived susceptibility and severity, TTAT frames these perceptions through the lens of restraint, rather than proactive security engagement (Moody et al., 2018; Xin et al., 2021). Consequently, integrating PMT and TTAT provides a comprehensive framework for understanding both protective behaviour adoption (mitigating passive risks) and risky behaviour avoidance (preventing active risks). This dual theoretical perspective informs the current study's approach to measuring perceived threat across both active and passive risk types.

From a behavioural perspective, perceived threat acts as a motivational filter, prompting caution when a behaviour is identified as threatening (Hooper & Blunt, 2020). This caution manifests in behaviours like double-checking information, updating security protocols, or avoiding actions that could compromise their digital safety (Ogbanufe et al., 2021, 2023). Nevertheless, these cautious responses can be overridden by competing factors like curiosity, task urgency, or external pressures, particularly in active risk-taking scenarios (Chowdhury et al., 2020). Additionally, repeated engagement in risky behaviours without negative consequences can lead to habituation, reducing the perceived threat and increasing the likelihood of continuing these behaviours (Fatoki et al., 2024; Verplanken & Aarts, 1999). When threats are perceived as distant or unlikely, individuals are more likely to dismiss potential hazards and act impulsively, prioritising convenience over caution (House & Raja, 2020; Moody et al., 2018; Vedadi et al., 2021). As risk-taking behaviour persists without immediate repercussions, initial threat impact weakens, and neutralisation strategies become more ingrained (Padayachee, 2015). This gradual erosion of perceived threat, coupled with stronger neutralisation, diminishes the motivational force of warnings and security reminders.

Ultimately, threat perception is neither static nor uniformly effective. Its influence fluctuates based on how individuals interpret specific behaviours, prevailing contextual factors, and repeated risk exposure. Recognising this inherent variability is essential when designing cybersecurity awareness initiatives aimed at fostering genuine relevance.

2.3 Neutralisation

While threat perception aims to deter risky behaviours, its influence can be attenuated by neutralisation strategies. Derived from Sykes and Matza (1957), neutralisation refers to cognitive techniques individuals employ to rationalise deviant behaviour, temporarily suspending moral responsibility to violate norms while maintaining a positive self-concept.

In cybersecurity, neutralisation allows employees to justify non-compliance with security

policies (Barlow et al., 2018; Siponen & Vance, 2010). Neutralisation typically involves reflective, deliberate reasoning, where individuals justify non-compliance with thoughts like "*I know this is against the policy, but the risk feels minimal in this case*". When non-compliance goes unnoticed or without consequences, these justifications can become routinised and automatic (Verplanken & Aarts, 1999). While neutralisation can reduce cognitive dissonance in both active and passive risk-taking scenarios, its manifestation may differ.

For active risk behaviours, neutralisation often takes the form of convenience-based justifications that downplay severity. For instance, employees may knowingly use USB devices against policy, rationalising actions with statements like "*I've done this before without issues, so the risk is low*" or "*I don't have the time to upload files to the cloud, and this is faster*" (Hwang et al., 2016; Prabhu & Dell, 2025a). Even with awareness of potential risks, simplicity and convenience can override security concerns (Sykes & Matza, 1957). In such cases, neutralisation techniques reduce psychological discomfort from knowingly engaging in risk-taking (Gruber & Schlegelmilch, 2014). For passive risk-taking, neutralisation tends to manifest as procrastination or neglect that minimises the perceived urgency. Justifications such as "*It's unlikely someone will steal my password*" or "*I'll change it later*" excuse inaction and downplay potential risk.

The interplay between neutralisation and threat perception is critical. As individuals repeatedly engage in risky cybersecurity behaviours, especially without immediate negative consequences, they become susceptible to neutralisation (Maruna & Copes, 2005). As individuals become accustomed to these patterns, justifications become more ingrained and automatic, effectively lowering the threshold for non-compliance with security protocols (Fatoki et al., 2024). This routine justification process can occur across both active and passive risk-taking, but manifests differently. In active risk-taking contexts, repeated rule-breaking may be reframed as efficient or harmless. In passive risk-taking contexts, recurring neglect fosters complacency, as inaction becomes normalised and the perceived urgency of security fades.

While neutralisation has been widely used to explain deviant behaviour, its specific role in distinguishing the psychological underpinnings of active and passive risk cybersecurity behaviours remains underexplored. Understanding whether neutralisation more effectively justifies deliberate policy violations or excuses inaction is crucial for addressing the psychological mechanisms influencing compliance.

3 Theoretical Framework

Our conceptual framework posits that both *threat perceptions* and *neutralisation* are key psychological antecedents to employees' *cybersecurity behavioural intentions.* The framework specifically accounts for both active and passive forms of risk-taking, ultimately determining whether employees adopt caution or risky practices. In this model, threat perceptions are expected to motivate caution and compliance, whereas neutralisation facilitates justification for non-compliance. By encompassing both compliant and risky behavioural pathways, this framework offers a comprehensive lens for understanding employee cybersecurity actions.

Cybersecurity behavioural intentions refer to deliberate, goal-directed inclinations to either adhere to or disregard secure practices (Ajzen, 1985). These intentions are shaped by employees' cognitive evaluations of risk and justification for deviance, and are widely recognised as proximal predictors of actual behaviour in information security contexts (e.g.,

(Barlow et al., 2018; Prabhu & Dell, 2025a; Vance et al., 2020; Willison et al., 2018)).

Within this framework, perceived threat is central. Studies report its significant impact, whether as individual components like susceptibility and severity (e.g., (Hooper & Blunt, 2020; Johnston et al., 2023; Vedadi et al., 2021)) or as a unified construct (e.g., (Carpenter et al., 2019; Moody et al., 2018; Rajab & Eydgahi, 2019)). This study adopts the latter, focusing on perceived threat as a holistic risk appraisal to capture broader employee behavioural patterns. This perspective captures how individuals often respond to an overall sense of threat, integrating both cognitive and emotional responses (Liang & Xue, 2009). It allows for a more parsimonious examination of its influence across both active and passive risk-taking. Employees are generally more likely to avoid behaviours when they perceive a high susceptibility to a severe threat (Aigbefo et al., 2022). Perceived threats are powerful motivators, compelling individuals to adjust their behaviour based on the intensity and immediacy of the risk they face (Chowdhury et al., 2020; Ogbanufe et al., 2021, 2023). However, threat impact can diminish with familiarity or abstractness, leading to a gradual decline in caution and increased likelihood of non-compliant actions (Fatoki et al., 2024). PMT posits that threat perceptions enhance compliance motivation, whereas TTAT links them to avoidance motivation (Carpenter et al., 2019). Given the consistent empirical evidence demonstrating a significant influence of threat perceptions on security-related intentions, we hypothesise:

H1: *Perceived threat positively influences cybersecurity intentions.*

Even when aware of potential threats, individuals may engage in neutralisation, self-justifying non-compliant actions (Vance et al., 2020). These rationalisations not only preserve a positive self-image but also diminish perceived risks (Fatoki et al., 2024) associated with both active and passive risk-taking. Offenders may convince themselves that their behaviour is harmless, despite policy violation (Siponen & Vance, 2010). For example, an employee might justify not encrypting a laptop hard drive by rationalising that "no one will be harmed by this oversight".

Consistent with this theoretical understanding, empirical research demonstrates a significant negative impact of neutralisation on security behavioural intentions. Studies, including Barlow et al. (2018), Moody et al. (2018), and Willison et al. (2018), report a significant negative influence of neutralisation on security intentions. Given consistent evidence that neutralisation enables the persistence of non-compliant behaviour, we hypothesise:

H2: *Neutralisation negatively impacts cybersecurity intentions.*

Beyond individual effects of perceived threat and neutralisation, understanding their relative influence on cybersecurity behaviours is crucial. Neutralisation often exerts a stronger impact than perceived threats, enabling individuals to psychologically bypass risk awareness and justify risk-taking behaviours (Barlow et al., 2013). While perceived threat is generally considered a primary deterrent, prior research indicates it may not always suffice to prevent non-compliant behaviour, especially when rationalisations diminish the perceived risk (Moody et al., 2018).

Threats often feel abstract, distant, or hypothetical, especially in familiar work routines, whereas neutralisation operates in the immediate decision context, providing cognitive justifications that make risk-taking behaviours feel acceptable in the moment (Prabhu & Dell, 2025a). For example, an employee might acknowledge the general threat of using personal USB devices but still do so, rationalising it with "*it's just this once*" or "*this data is not sensitive*". Such justifications effectively allow convenience to override their awareness of potential risk

(Barlow et al., 2013; Siponen & Vance, 2010). Thus, this study proposes that neutralisation may play a more dominant role than the often-abstract perception of threat in sustaining risky cybersecurity intentions.

H3*: Neutralisation has a larger effect than perceived threat for everyday risky cybersecurity intentions.*

The impact of threat perception and neutralisation is also likely to differ across active and passive risk types. In active risk scenarios, perceived threat is often more explicit because individuals knowingly act against prescribed policies and consciously consider the potential consequences (Liang & Xue, 2009). However, the intensity of this perceived threat can vary due to normalisation or habitual use, leading individuals to view it as low-risk. In such contexts, individuals often employ neutralisation strategies like *"Everyone here does this"* or "*It's never been a problem*", employed to alleviate the psychological discomfort of knowingly violating security protocols.

Conversely, passive risk scenarios typically involve subtler threat perceptions. Since this behaviour involves inaction rather than overt violation, individuals may not perceive an immediate urgency or significant risk (Rogers, 1975). For example, delaying a security task like installing software updates may seem low-risk, often accompanied by a mindset of "*I'll do it soon*" (Arend et al., 2020). Such justifications support inaction without directly challenging norms and typically do not require strong, explicit justifications. While neutralisation may still be present, it tends to be more implicit and less deliberate, reducing urgency and enabling procrastination (Padayachee, 2015).

Thus, in active risk scenarios, threats are often explicitly perceived, and neutralisation's influence in overriding threat perception is likely more pronounced. In contrast, in passive risk scenarios, threats are subtler, and neutralisation is a less overt mechanism, often without requiring strong justifications. Given these theoretical distinctions, this study proposes the comparative hypothesis:

H4: *Neutralisation has a larger effect on active risk than passive risk cybersecurity intentions.*

The distinction between active and passive risk behaviours leads to a critical question: *Is one type of cybersecurity risk-taking more prevalent than the other?* Psychological principles offer insight into this disparity. The default effect (Samuelson & Zeckhauser, 1988), alongside avoidance, omission bias, default bias (Baron & Ritov, 2004), inaction inertia (Tykocinski & Pittman, 1998), and procrastination, collectively explain human tendency toward inaction despite potential risks. This tendency to maintain the status quo in passive risk behaviours is amplified by the lower cognitive effort required compared to the deliberate actions of active risk behaviours (Keinan & Bereby-Meyer, 2012). The comfort of habit, the lower perceived immediate risk, and inherent ease of inaction further contribute to the expectation that passive risk-taking behaviours will be more frequent than the more deliberate and cognitively demanding active risk-taking behaviours. Therefore, we propose:

H5: *Passive risk-taking is more frequent than active risk-taking cybersecurity behaviours.*

These five hypotheses form the core propositions of this study. Hypotheses H1 through H4 form the research model (as depicted in Figure 1) and H5 is a descriptive hypothesis about the risk context that will be tested separately.

We acknowledge that factors such as gender and work experience could influence individuals' risk-taking behaviours. To ensure observed effects of threat perception and neutralisation

were independent of these demographic characteristics, our analysis controlled for gender and work experience as covariates. The following section outlines the methodology used to test these hypotheses.

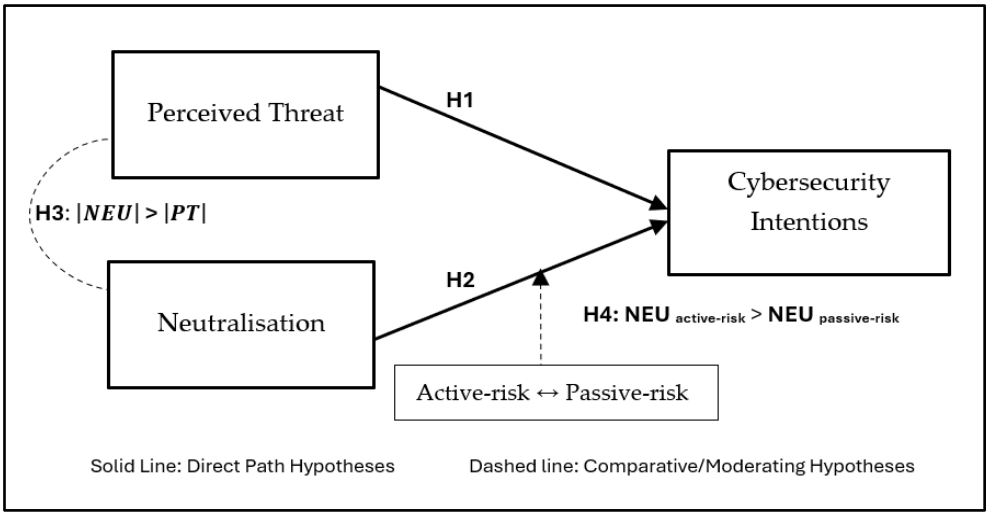

Figure 1: Research Model

4 Methodology

4.1 Research Design and Approach

This study used a quantitative approach to investigate threat perception and neutralisation as antecedents of employee cybersecurity behavioural intentions. Using a positivist paradigm, a survey design collected data from a broad sample of employees. This approach allowed examination of relationships between variables at a single point in time.

4.2 Cybersecurity Behaviour Selection

To understand how non-malicious employees contribute to cybersecurity risks through discretionary choices, this study examines four common, employee-controlled behaviours identified in industry reports (DBIR, 2024; Honeywell, 2024; Netskcope, 2025; ProofPoint, 2023) for their prevalence and documented risk impact.

- *Using USB devices (Behaviour 1 or B1) – Active risk-taking:* Plugging an external USB device into a work computer is a deliberate action that can introduce malware or data exfiltration risks. Honeywell's *2024 USB Threat Report* found that 51% of malware attacks target USB devices, a six-fold increase since 2019 (Honeywell, 2024).
- *Opening unknown links (Behaviour 2 or B2) – Active risk-taking:* Clicking on hyperlinks from untrusted sources (e.g., phishing emails, unverified websites) requires explicit action, which can lead to malware infection or credential theft. Netskope's *2024 Cloud & Threat Report* reported a 190% year-over-year rise in enterprise users clicking phishing links (Netskcope, 2025).
- *Failing to create new passwords (Behaviour 3 or B3) – Passive risk taking:* (henceforth reusing passwords) reusing passwords instead of creating unique ones for different accounts is a passive risk, as vulnerability arises from this omission, potentially leading to widespread account compromise if one account is breached. Cybernews reported that 94% of the 19 billion passwords leaked between 2024 and 2025 were reused or duplicates (TOI, 2025).

- *Failing to secure portable devices (Behaviour 4 or B4) – Passive risk-taking:* (henceforth unsecured devices) omission of security measures (e.g., screen locks, encryption) on portable devices (e.g., laptops, tablets, smartphones) with organisational data. This exemplifies passive risk-taking, as this lack of a protective action increases the risk of unauthorised access or data loss if the device is lost or stolen. Kensington's *2025 survey* found that 46% of organisations experienced breaches due to unsecured devices (Kensington, 2025), echoing *DBIR 2024* findings that laptops continue to be prominent assets in loss and theft incidents (DBIR, 2024).

These behaviours were selected to capture both active and passive forms of risk-taking, offering a balanced basis for examining how threat perception and neutralisation shape cybersecurity decisions.

4.3 Procedure

To ensure objective measurement and statistical analysis, and minimise researcher bias, this study employed a quantitative research design (Bagozzi, 2011) using a web-based Qualtrics survey. The survey method was chosen for its suitability in behavioural cybersecurity research and its capacity to measure relationships between key constructs: Cybersecurity Intention (CSI), Perceived Threat (PT), and Neutralisation (NEU). Each construct was measured using three items (refer to Appendix A). Where possible, validated items from prior studies were adapted to fit the specific research context.

4.3.1 Survey Design

Four versions of the survey were created, one for each of the four behaviours under investigation. Each version comprised three blocks: Block 1 collected self-reported behavioural tendencies for the four chosen behaviours. Positioned first, this mitigated order effects and social desirability bias by collecting these responses before introducing theoretical concepts (Bagozzi, 2011). Block 2 contained construct items (PT, NEU, CSI) tailored to one of the four active or passive risk behaviours, with item presentation order randomised. It used a 7-point Likert scale ranging from "Strongly Disagree" to "Strongly Agree". Block 3 collected demographic details, like gender and work experience. Blocks 1 & 3 were identical for all participants.

4.3.2 Survey Measures

Consistent with PMT and TTAT (Section 2.2), perceived threat was measured across both risk types using consistent item formats tailored to behaviour. For example, participants responded to items such as "*My organisation's data is susceptible to illegal access when I <behaviour>*", with the <behaviour> contextually adapted (e.g., "*... when I use USB devices*", for active, and "*... when I do not encrypt my laptop*" for passive). This uniform structure, combined with behaviour-specific phrasing, ensured conceptual clarity and methodological consistency, facilitating valid comparisons.

4.3.3 Survey Deployment

The survey received low-risk ethical approval from the author's university Ethics Office. Participants were recruited via Prolific and assigned to complete only one version of the survey, corresponding to a single cybersecurity behaviour. This design prevented potential priming effects from exposure to all behaviours, ensuring responses were specific to the present risk context.

The survey commenced with an informed consent section detailing voluntary participation, anonymity, confidentiality, and absence of foreseeable risks. To mitigate social desirability bias, the anonymous survey framed security behaviours as commonplace, rather than exceptional, reducing the tendency for participants to present themselves in an overtly positive light (Bagozzi, 2011). The eligibility criteria required individuals to be employed and to use computers at work. Those not meeting the criteria were informed and directed to the end of the survey.

4.4 Participants and Sampling

A total of 609 survey responses were collected (B1: 154, B2: 149, B3: 162, B4: 144). To ensure data quality, responses completed in under 7 minutes or with over 50% blank answers were removed, resulting in a final sample of 490 valid responses (B1: 118, B2: 128, B3: 120, B4: 124), representing an 80.46% overall acceptance rate. An *a priori* power analysis conducted using G*Power 3.1 indicated a sample size of 111 would suffice to detect an effect size of .3 (power=.8, significance=05), a threshold our final sample size exceeded.

The final sample of 490 participants had an almost even gender distribution: 49.8% (n=244) identified as male, 49.8% (n=244) as female, and 0.4% (n=2) as other. The majority were highly experienced, with 65.5% (n=321) reporting 12 or more years of work experience. A detailed breakdown of the demographic profile is provided in Appendix B.

4.5 Measurement Validation

All statistical analyses were performed using IBM SPSS Statistics 29 and IBM SPSS AMOS 29. Table 2 shows the validity fit and model fit summary.

Validity Measures									
Measure		**Threshold value**		**B1 (n=118)**		**B2 (n=128)**	**B3 (n=120)**		**B4 (n=124)**
cmin/df		>=1 and <=3		1.176		1.443	1.752		1.789
CFI		>0.950		0.991		0.966	0.962		0.951
RMSEA		<0.050		0.039		0.048	0.049		0.046
PCLOSE		>0.050		0.714		0.163	0.117		0.214
Model Fit Summary									
	Mean	**St. Dev**	**CR**	**AVE**	**MSV**	**MaxR(H)**	**PT**	**NEU**	**CSI**
B1 – Using USB devices									
PT	5.577	1.248	0.894	0.585	0.192	0.897	**0.765**		
NEU	4.454	1.822	0.951	0.763	0.350	0.968	-0.438	**0.874**	
CSI	5.367	1.917	0.959	0.887	0.350	0.960	0.436	-0.592	**0.942**
B2 – Opening Unknown Links									
PT	6.212	0.941	0.827	0.504	0.202	0.904	**0.674**		
NEU	2.698	1.704	0.958	0.792	0.382	0.973	-0.446	**0.890**	
CSI	6.401	1.110	0.839	0.635	0.382	0.841	0.449	-0.618	**0.797**
B3 – Reusing Passwords									
PT	5.648	1.777	0.887	0.576	0.354	0.918	**0.759**		
NEU	3.714	1.762	0.955	0.780	0.354	0.971	-0.595	**0.883**	
CSI	5.635	1.388	0.936	0.829	0.211	0.936	0.459	-0.437	**0.911**
B4 – Unsecured Portable Devices									
PT	5.826	1.203	0.855	0.505	0.203	0.891	**0.711**		
NEU	2.639	1.472	0.935	0.707	0.303	0.956	-0.369	**0.841**	
CSI	6.169	1.003	0.826	0.614	0.303	0.848	0.450	-0.550	**0.784**

Table 2: *Validity Fit and Model Fit Summary*

4.5.1 Reliability and Validity Assessment

Composite Reliability (CR) values for all constructs exceeded the recommended threshold of .700, ranging from 0.826 to 0.959. Maximal Reliability MaxR(H) values were also consistently high, further supporting scale reliability.

Convergent validity was supported by Average Variance Extracted (AVE) values exceeding the threshold of .50 (0.504 to .887), indicating over 50% variance in items is explained by their constructs. *Discriminant validity* was assessed by comparing AVE with the Maximum Shared Variance (MSV). For each construct, the $\sqrt{AVE}$ (bolded on the diagonal for PT, NEU, and CSI in Table 2) was greater than its highest correlation with any other construct. These findings confirm distinctness and unique measurements, thereby supporting adequate discriminant validity across all four behavioural contexts.

4.5.2 Common Method Bias (CMB)

CMB was assessed using three established methods. First, Harman's single-factor test revealed that no single factor accounted for more than 50% of the total variance across behaviours (34.73%, 34.33%, 35.45%, 28.78%). Second, the Common Latent Factor (CLF) technique was applied. Finally, the marker variable approach using gender as the marker was applied to examine the measurement model. The results from all three methods provided no evidence of significant CMB.

4.5.3 Control variables

Hierarchical multiple regression assessed the effects of age and work experience on cybersecurity intentions for each behaviour.

In all studies, Step 1, neither gender nor work experience significantly predicted cybersecurity intentions – B1 ($F(2,115)=.523$, $p=.594$, $R^2=.009$); B2 ($F(2,125)=.71$, $p=.495$, $R^2=.011$); B3 ($F(2,117)=1.51$, $p=.224$, $R^2=.025$); B4 ($F(2,121)=.032$, $p=.969$, $R^2=.001$). However, in Step 2, adding perceived threat and neutralisation resulted in significant models for all behaviours – B1 ($F(4,113)=16.860$, $p<.001$, $R^2=.374$); B2 ($F(4,123)=18.96$, $p<.001$, $R^2=.381$); B3 ($F(4,115)=11.12$, $p<.001$, $R^2=.279$); B4 ($F(2,119)=14.857$, $p<.001$, $R^2=.333$). These findings indicate that theoretical predictors (PT and NEU) accounted for a substantial proportion of the variance in cybersecurity intentions, while control variables (gender and work experience) did not significantly contribute.

5 Results

This section presents the findings from the data analysis, including descriptive statistics, measurement model assessment, and hypothesis testing results.

5.1 Descriptive Statistics and Correlations

This subsection provides an overview of study variables and the observed engagement levels. The sample's demographic profile (gender, work experience) is detailed in *Section 4.2. Participants and Sampling*, with a complete breakdown in Appendix B.

Table 2 presents the mean, standard deviation, and correlations for all latent constructs (CSI, PT, NEU). The values revealed that PT and CSI generally had high mean scores, while NEU exhibited more varied means across the four behaviours. All constructs demonstrated adequate variability in responses. Preliminary correlation analysis showed expected relationships, providing initial associations consistent with the proposed theoretical

framework.

5.1.1 Behavioural Frequencies

Participants reported the engagement frequency for all four behaviours using a scale from never to always (*never, rarely, sometimes, quite often, always*). Figure 2 illustrates these reported tendencies, revealing each behaviour's observed prevalence within the sample, which forms the basis for examining H5 regarding passive versus active risk behaviour frequency.

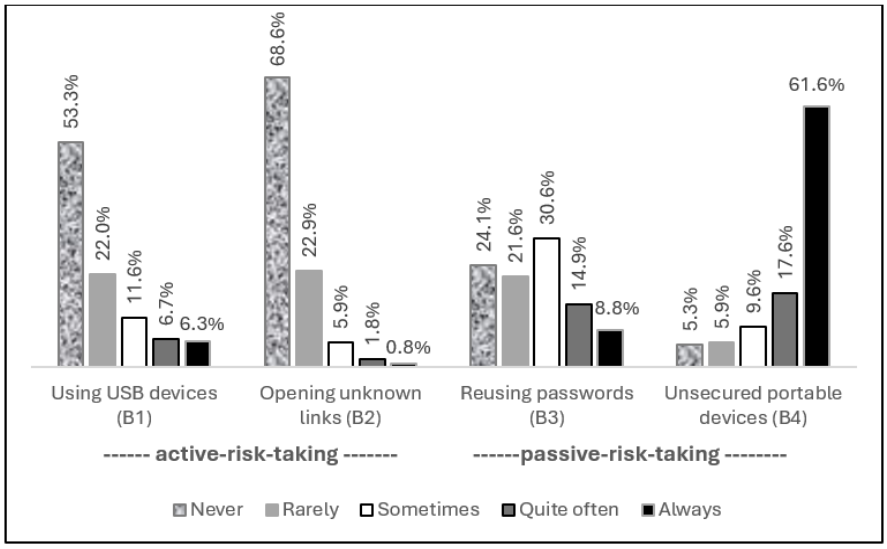

Figure 2: Frequency of engagement in the four cybersecurity behaviours (N=490)

A notable finding is the high caution regarding opening unknown links, an active risk behaviour, with 68.6% (336) of participants reporting *never* doing so, compared to only four reporting doing it *always*. Conversely, the most prevalent risk-taking behaviour appears to be the passive risk behaviour of failing to secure portable devices, with a significant 61.6% (302) admitting they *always* neglect this measure. Overall, active risk behaviours (using USB devices and opening unknown links) are self-reported as occurring significantly less frequently than passive risk behaviours (reusing passwords and unsecured portable devices).

5.2 Hypothesis Testing

Hypothesis	β	f^2	C.R.	p-value	Z-value (H3)	H4	H5
B1 – Using USB devices (R2 0.389)							
H1: PT → CSI	0.219	0.064	2.348	0.019 (s)			
H2: NEU → CSI	-0.496	0.326	-5.545	*** (s)	4.051 (s)		
B2 – Opening unknown links (R2 0.419)						(s)	
H1: PT → CSI	0.216	0.065	2.236	0.025 (s)			
H2: NEU → CSI	-0.521	0.423	-5.247	*** (s)	5.721 (s)		
B3 – Reusing passwords (R2 0.252)							(s)
H1: PT → CSI	0.308	0.082	2.465	0.014 (s)			
H2: NEU → CSI	-0.253	0.050	-2.336	0.019 (s)	5.251 (ns)~		
B4 – Unsecured portable devices (R2 0.373)						(s)	
H1: PT → CSI	0.286	0.121	2.626	0.009 (s)			
H2: NEU → CSI	-0.445	0.282	-4.339	*** (s)	5.948 (s)		

B1, B2 are active-risk behaviours, B3, B4 are passive-risk behaviours

~ opposite direction, **H3:** NEU > PT, **H4:** $NEU_{active\_risk} > NEU_{passive\_risk}$, **H5:** $Frequency_{passive\_risk} > Frequency_{active\_risk}$

Table 3: Hypothesis Results

To evaluate the proposed relationships, the structural model encompassing H1 and H2 was tested for each of the four cybersecurity behaviours. Hypotheses were considered supported (s) if their corresponding *p*-value was below the .05 significance level. The R^2 values were 38.9% for B1, 41.9% for B2, 25.2% for B3, and 37.3% for B4. Table 3 presents a complete summary of the hypothesis testing results.

To assess the strength and statistical significance of the hypothesised relationships, standardised regression coefficients (β) and their *p*-values are reported. Critical ratios (C.R.) further indicate the statistical significance of each structural path. Additionally, to provide insight into the practical significance, Cohen's f^2 was also considered, with values of .02, .15, and .35 corresponding to small, medium, and large effect sizes, respectively (Cohen, 2013).

Hypothesis 1 (H1) and Hypothesis 2 (H2):

H1 and H2 were supported across all behaviours. For B1 (using USB devices), perceived threat (β=.219, *p*=.019) positively influenced cybersecurity intentions, while neutralisation (β=–.496, *p*<.001) had a significant negative effect. Similarly, for B2 (opening unknown links), perceived threat (β=.216, *p*=.025) and neutralisation (β=–.521, *p*<.001) significantly influenced intentions.

For B3 (reusing passwords), both perceived threat (β=.308, *p*=.014) and neutralisation (β=–.253, *p*=.019) significantly influenced intentions. For B4 (unsecured portable devices), perceived threat (β=.286, *p=.009*) and neutralisation (β=–.445, *p*<.001) were both significant predictors of intentions.

These findings consistently support H1 and H2, indicating that both the perception of threat and use of neutralisation strategies play crucial roles in shaping employees' cybersecurity intentions across the active and passive risk contexts.

Hypothesis 3 (H3):

H3 posited that neutralisation would exert a larger impact on cybersecurity intentions compared to perceived threat. To evaluate this comparative influence, two complementary methods were employed: (1) an examination of Cohen's f^2 effect sizes to assess practical significance, and (2) a Z-test on the unstandardised regression coefficients to assess the statistical significance of the difference in their effects on cybersecurity intention. The Z-test used composite mean scores for each construct derived from the multiple regression analysis. A *Z*-value greater than 1.96 indicated a statistically significant difference at p<.05, while a Z-value exceeding 2.58 indicated significance at p<.001 (Field, 2024). The formulas and detailed calculations for Cohen's $f^2$and the Z-test are provided in Table 4.

The results, as summarised in Table 4, provide partial support for H3. For B1, neutralisation exhibited a medium to large effect size (f^2=.326), considerably larger than the small effect of perceived threat (f^2=.064). This difference was statistically significant, as confirmed by a Z-test (*Z=4.051, p<.001*), supporting H3. Similarly, for B2, neutralisation showed a notably larger effect size (f^2=.423) compared to the small effect of perceived threat (f^2=.065), further supporting H3 (*Z=5.721.051, p<.001*). For B4, neutralisation also displayed a larger effect size (f^2=.282) than the perceived threat (f^2=.121), with this difference being statistically significant (*Z=5.9484, p<.001*), providing additional support for H3.

(a) Cohen's f^2

$$f^2 = \frac{R^2{}_{inc} - R^2{}_{exc}}{1 - R^2{}_{exc}}$$

R^2_{inc}: R^2 of the full model, with predictor of interest

R^2_{exc}: R^2 of the model without predictor of interest

		PT			NEU		
	R^2_{inc}	R^2_{exc}	f^2	effect size	R^2_{exc}	f^2	effect size
B1 – using USB devices	.389	.350	.064	small	.190	.326	medium
B2 – opening unknown links	.419	.381	.065	small	.173	.423	large
B3 – reusing passwords	.252	.191	.082	small	.215	.050	small
B4 – unsecured portable devices	.373	.297	.121	small	.196	.282	medium

(b) Z-Test Results

$$Z = \frac{\beta_{PT} - \beta_{NEU}}{\sqrt{SE_{PT}{}^2 + SE_{NEU}{}^2 - 2 \times r \times SE_{PT} \times SE_{NEU}}}$$

SE_{PT}: Standard Error PT

SE_{NEU}: Standard Error NEU

β_{PT}: unstandardised regression coefficient PT

β_{NEU}: unstandardised regression coefficient NEU

r: correlation between PT and NEU

	β_{PT}	B_{NEU}	SE_{PT}	SE_{NEU}	r	Z	outcome
B1 – using USB devices	.309	-.525	.126	.086	-.420	4.0516	p<.001
B2 – opening unknown links	.278	-.306	.096	.053	-.462	5.7217	p<.001
B3 – reusing passwords	.337	-.209	.112	.075	-.526	5.2514	p<.001
B4 – unsecured portable devices	.249	-.279	.070	.057	-.380	5.9484	p<.001

Table 4: Cohen's f^2 and Z-Test Results (for H3)

In contrast, for B3, both perceived threat (f^2 =.082) and neutralisation (f^2 =.050) showed relatively small effect sizes. Neutralisation showed a slightly lower practical impact than perceived threat for this specific behaviour. Despite these modest overall effects, a statistically significant difference between the predictors was observed (*Z=5.251, p<.001*), indicating that perceived threat had a stronger relative contribution to compliance intentions for this behaviour, contrary to H3's prediction.

Therefore, H3, which posited that neutralisation would have a larger effect than perceived threat, was supported for B1, B2, and B4, but not for B3; thus, H3 was partially supported.

Hypothesis 4 (H4):

H4 proposed that neutralisation would exert a stronger influence on active risk-taking compared to passive risk-taking behaviours. To test this comparative hypothesis, a two-pronged approach was used: (1) comparing Cohen's f^2 effect sizes of neutralisation across these behaviour-types, and (2) conducting Z-tests on the unstandardised regression coefficients for neutralisation.

Two sets of behavioural pairings were used for the Z-tests: active vs. passive (B1–B3, B2–B4) and an alternative pairing (B1–B4, B2–B3). These pairings enabled direct comparison of NEU's impact on active risk vs. passive risk behaviours. The Z-test formula for grouped comparisons (Field, 2024) and detailed calculations are provided in Table 5.

$$Z = \frac{\beta_1 - \beta_2}{\sqrt{SE_1{}^2 + SE_2{}^2}}$$

SE_1: Standard Error behaviour 1

SE_2: Standard Error behaviour 2

β_1: unstandardised regression coefficient NEU for behaviour 1

β_2: unstandardised regression coefficient NEU for behaviour 2

Pairings	Z-value of the first set	Z-value of second set
B1-B3 and B2-B4	$\mathbf{Z}_{\text{B1-B3}} = \frac{-.525--.209}{\sqrt{.086^2+.075^2}} = \mathbf{4.9263}$	$\mathbf{Z}_{\text{B2-B4}} = \frac{-.306--.279}{\sqrt{.053^2+.057^2}} = \mathbf{2.1111}$
B1-B4 and B2-B3	$\mathbf{Z}_{\text{B1-B4}} = \frac{-.525--.279}{\sqrt{.086^2+.057^2}} = \mathbf{4.8072}$	$\mathbf{Z}_{\text{B2-B3}} = \frac{-.306--.209}{\sqrt{.053^2+.075^2}} = \mathbf{3.3913}$

Table 5: Z-Test (for H4)

Effect size comparison: An examination of Cohen's f^2values revealed nuanced patterns for both perceived threat and neutralisation. Perceived threat consistently demonstrated a positive influence across all behaviours, with slightly larger effect sizes observed for passive risk behaviours (B3: f^2=.082, B4: f^2=.121) compared to active risk behaviours (B1: f^2=.064, B2: f^2=.065). This suggests a potentially greater responsiveness of passive risk behaviours to threat perceptions.

In contrast, neutralisation consistently exerted a strong negative influence across all behaviours, with notably larger effect sizes for active risk behaviours (B1: f^2=.326, B2: f^2=.423) than for passive risk behaviours (B3: f^2=.050, B4: f^2=.282). This finding indicates a more substantial role for neutralisation in undermining intentions related to active risks. These initial findings support H4.

Z-test comparisons: To further validate the stronger influence of neutralisation for active risk behaviours (B1, B2) compared to passive risk behaviours (B3, B4), two sets of Z-tests were conducted, comparing the unstandardised regression coefficient across behaviour pairs.

- ***B1–B3 and B2–B4 pairings:*** The Z-test comparing the impact of neutralisation in B1 and B3 yielded a significant result (Z=4.926, p<.001). This indicates that neutralisation had a significantly stronger effect in active risk behaviour B1 compared to passive risk B3. Similarly, the comparison between B2 and B4 also showed a significant difference (Z=2.11, p<.05), further supporting the stronger influence of neutralisation on active risk behaviours.
- ***Alternative B1–B4 and B2–B3 pairings:*** The Z-test comparing the impact of neutralisation in B1 and B4 revealed a significant result (*Z*=4.807, p<.001). This confirmed that neutralisation had a greater impact on active risk behaviour B1 than on passive risk behaviour B4. Likewise, the comparison of B2 and B3 also yielded a significant Z-value (*Z*=3.391, p<.001), reinforcing the finding.

Both sets of pairings, (B1-B3, B2-B4) and (B1-B4, B2-B3), consistently demonstrated that neutralisation exerted a significantly stronger influence on active risk behaviours compared to passive risk behaviours. These findings are consistent with the effect size comparisons, where neutralisation showed larger values for active risk behaviours. Collectively, these findings provide strong support for H4.

Hypothesis 5 (H5):

H5 posited that passive risk-taking behaviours are more frequent than active risk-taking behaviours. To examine this difference in behavioural frequency, a Wilcoxon Signed-Rank Test was employed. This non-parametric test was chosen due to the repeated-measures (within-subjects) design, where the same participants reported on the frequency of all four

behaviours (Wilcoxon, 1992). The Wilcoxon test allowed for a robust comparison of whether passive risk-taking was performed significantly more frequently than active risk-taking.

In terms of self-reported behavioural tendency, Figure 2 visually illustrates the distinct patterns observed. Passive risk-taking behaviours (B3, B4) were indeed performed more frequently, with 8.8% (B3) and 61.6% (B4) of participants reporting "always" performing these behaviours. In contrast, active risk-taking behaviours showed much lower frequencies, with only 6.3% (B1) and 0.8% (B2) reporting to "always" perform them. These preliminary descriptive patterns strongly align with H5. Interestingly, these descriptive patterns align with previously discussed findings: perceived threat was also stronger for the passive risk behaviours (B3, B4), whereas neutralisation was more pronounced in the less frequent active risk behaviours (B1, B2).

To statistically confirm the observed descriptive trends, a Wilcoxon Signed-Rank Test was conducted. This involved comparing the mean frequency score for each participant across the two active risk behaviours (B1, B2) against the two passive risk behaviours (B3, B4). The results revealed a statistically significant difference between the two categories, with passive risk behaviours being reported as performed significantly more often than active risk behaviours (Z=18.18, $p<.001$). This statistical evidence supports H5, indicating that individuals are more likely to engage in passive forms of risk-taking behaviour compared to active ones.

In summary, hypotheses H1, H2, H4, and H5 were supported, whereas H3 was only partially supported due to the comparable effect sizes of perceived threat and neutralisation in B3.

6 Discussion

This study empirically examined how perceived threat and neutralisation differentially influence active and passive cybersecurity risk behaviours. Understanding these distinct psychological mechanisms is crucial for designing effective interventions that can promote consistent security practices. The findings, derived from an analysis of four common cybersecurity behaviours – using USB devices (B1), opening unknown links (B2), reusing passwords (B3), and unsecured portable devices (B4) – are discussed below, highlighting their theoretical and practical implications.

H1, H2: Consistent with H1, perceived threat significantly predicted compliance intentions across all four behaviours. This finding, underscored by the consistently high mean scores, reinforces the foundational role of risk appraisal in shaping cybersecurity practices, aligning with PMT, TTAT, and extant literature (e.g., (Hong et al., 2023; House & Raja, 2020; Johnston et al., 2023). Individuals intend compliant behaviour when they perceive the potential negative consequences of non-compliance as severe and personally relevant.

Similarly, H2, positing a negative influence of neutralisation, was consistently supported across all four behaviours. This finding affirms the pervasive role of neutralisation in facilitating risky choices. This aligns with prior research (e.g., (Barlow et al., 2018; Hwang et al., 2016; Siponen & Vance, 2010)), indicating neutralisation provides psychological "permission" to engage in behaviours otherwise perceived as non-compliant.

H3: The results of H3 demonstrate that neutralisation often holds greater psychological potency than perceived threat, emerging as a stronger predictor of compliance intentions across three of the four behaviours (B1, B2, B4). This suggests that even when employees are aware of threats, the immediate lure of convenience outweighs perceived, often distant, risk

(Hwang et al., 2016; Rogers, 1983). As Ajzen (1985) suggests, when a behaviour presents both desirable (e.g., convenience) and undesirable (e.g., risks) aspects, individuals often default to the most effortless option.

The exception was B3, where the effect size of neutralisation was marginally smaller than that of perceived threat for password reuse. This provides a key theoretical insight: pervasive messaging about password dangers may diminish rationalisations, making it harder to justify this well-understood risk.

A striking finding was observed for B2 (opening unknown links); while neutralisation exhibited the highest effect size, it was also the least frequently performed behaviour overall. This counterintuitive result suggests that while strong justifications might be readily "available" (e.g., curiosity, perceived harmlessness), powerful inhibiting factors may be individual (e.g., ethical values) or organisational (e.g., explicit policy enforcement, clear leadership messaging, robust security-aware workplace culture) that might override these rationalisations (Li et al., 2019). This highlights that the interplay between perception and neutralisation is complex and can be moderated by broader contextual and cultural elements.

H4: This study's novel contribution is its examination of the differing impact of perceived threat and neutralisation on active versus passive risk-taking. H4 was supported; neutralisation's impact was notably stronger in active risk scenarios. This suggests employees may engage in more intense rationalisation when performing an overt, risky action. Active behaviours might be viewed as a direct transgression, requiring more substantial psychological justifications to mitigate guilt or responsibility. In contrast, passive behaviours, being omissions rather than actions, might be seen as less direct or more socially acceptable, thus requiring less explicit justification (Arend et al., 2020).

In passive risk contexts, although perceived threat might initially raise awareness, its motivational influence may fade over time due to factors like neutralisation. This temporary waning of threat perception can allow neutralisation to become more dominant, enabling these passive behaviours to persist unchecked. Furthermore, the repeated performance or omission of behaviours can lead to automaticity and habit formation (Neves et al., 2025; Verplanken & Aarts, 1999). This habituation reduces the likelihood of conscious corrective actions, as individuals revert to ingrained responses. This provides a theoretical explanation for their higher frequency observed in this study, aligning with the theoretical perspectives on habit formation (Verplanken & Aarts, 1999) and neutralisation (Sykes & Matza, 1957). Thus, non-compliance mechanisms vary by risk-taking behaviour: neutralisation may exert a stronger, more explicit influence for active actions, while implicitly enabling procrastination and inaction in passive contexts.

H5: The results unequivocally corroborate H5, confirming a clear and statistically significant distinction: passive risk-taking (B3, B4) were reported as performed more frequently than active ones (B1, B2). This compelling finding suggests that frequent, seemingly minor omissions can collectively pose a significant security risk.

Two key observations emerge. First, although perceived threat was significant across both categories, its reported level was lower in the active risk contexts. This suggests that individuals may view these scenarios as less personally relevant or unlikely to materialise compared to passive risk-taking ones. Second, while neutralisation is prominent in both risk types, its effect was particularly pronounced in the less frequent active risk behaviours. This

indicates that even in the absence of strong threat perceptions, individuals can readily rationalise active risk-taking behaviours.

Despite stronger neutralisation effects in active risk behaviours, these actions were reported less frequently. The higher prevalence of passive risk-taking can be attributed to the self-reinforcing nature of inaction and delay. As individuals repeatedly postpone security measures without immediate negative outcomes, the behaviour becomes more familiar and acceptable (Neves et al., 2025). For instance, consistently ignoring software update prompts can develop an automatic disregard for such alerts, increasing vulnerability. Moreover, perceived success of past inaction can further normalise unsafe practices, lower risk sensitivity, and strengthen existing rationalisations for non-compliance.

Notably, failing to secure portable devices (B4) was reported as the most frequently performed behaviour. This finding, that the most frequent risk occurs despite high perceived threat and low neutralisation, suggests that factors like convenience and familiarity may override conscious security concerns. This persistence is often enabled by the organisational context; a lack of stringent policy enforcement or permissive management behaviour can inadvertently signal that these "minor" passive risks are acceptable omissions (Hooper & Blunt, 2020). This highlights the psychological tension between risk perception, justification, and convenience in shaping everyday organisational security behaviour.

Furthermore, password reuse (B3) exhibited a more uniform distribution across users, indicating broader acceptance and normalisation across a wide user spectrum, unlike behaviours that tend to cluster within a specific risk-taking profile. This poses a significant challenge for intervention strategies, necessitating a broad-based approach targeting general security awareness and policy adherence, rather than focusing solely on a small segment of highly negligent users.

6.1 Implications

This research offers a nuanced understanding of how threat perceptions and neutralisation differentially shape cybersecurity intentions across active and passive risk-taking behaviours.

This study advances the PMT and ToN framework by demonstrating that their respective predictors (threat appraisal and neutralisation) are not universally applicable but are context-specific, contingent upon the nature of the risk-behaviour. Specifically, we establish a novel boundary condition for PMT's efficacy, showing that threat perception's motivational power is more pronounced for passive risk behaviours, where convenience and habit dominate, than for active ones. This moves theoretical frameworks beyond treating risks as mere variants of general non-compliance and calls for differentiated models based on behaviour types.

Our finding that neutralisation consistently emerges as a stronger predictor of compliance intentions for active risk behaviours significantly expands the theoretical relevance of ToN in the cybersecurity domain. This suggests that deliberate active choices are driven more strongly by self-justifications than by threat avoidance. This insight directly challenges models that prioritise threat perception as the primary determinant across all security actions and aligns with the *National Institute of Standards and Technology Cybersecurity Framework's* (NIST CSF's) "Protect" and "Respond" functions, which advocate proactive mitigation of behavioural drivers rather than reliance on fear appeals alone (NIST, 2024).

The observed prevalence of passive risk behaviours lays the groundwork for integrating habit theory or theories of automaticity into cybersecurity risk models. By suggesting that passive

risks are deeply embedded in routines, our findings highlight a theoretical need to reconsider how familiarity may paradoxically reduce perceived urgency and inadvertently reinforce procrastination. This highlights the need for future models to consider the interplay between cognitive risk appraisal and non-cognitive, routine-based action.

6.1.1 Practical Implications

This research offers several actionable insights for practitioners aiming to improve cybersecurity compliance. Firstly, the demonstrated higher frequency of passive risk-taking behaviours underscores the need for proactive organisational strategies. To reduce these prevalent risks, organisations should re-engineer workflows to identify and eliminate opportunities for routine security bypass. This includes simplifying security protocols to reduce cognitive burden and defaulting to risky shortcuts, and critically, automating essential security tasks to remove total reliance on user action, and aligning with the NIST CSF's "Identify" and "Protect" functions (NIST, 2024).

Secondly, the finding that neutralisation often outweighs perceived threat suggests a limitation to purely fear-based security campaigns. Instead, organisations should implement context-aware interventions that directly address potential neutralisation at critical decision points (e.g., alerts before sending sensitive data) and leverage behavioural nudges to guide users towards secure choices in the moment.

Finally, the research reinforces the heterogeneity of employee engagement with cybersecurity risk. To foster more consistent security practices, organisations should adopt tailored interventions that integrate security seamlessly into existing work routines. Promoting reflective decision-making through targeted training (i.e., customising content, format, and examples to be directly relevant to employees' roles and daily tasks), aligning with the NIST CSF's "Protect" function, thereby reducing impulsive risk-taking and ensuring behavioural resilience and sustainability over time (NIST, 2024).

By strategically implementing these multifaceted approaches, organisations can effectively reduce both active and passive risk behaviours and significantly strengthen their overall cybersecurity resilience.

6.2 Future Research

Based on this study's insights into the psychological mechanisms of active and passive cybersecurity risk-taking, future research could explore the following avenues.

First, this study conceptualised perceived threat as the second-order construct, integrating susceptibility and severity to reflect employees' overall risk appraisal. Future studies could explore these components individually to identify how each influences active and passive risk-taking behaviours to reveal more granular insights.

Second, to enhance validity and generalisability, future studies must specifically address the limitations of self-reported data by adopting a multi-method research. Given the encouragingly high mean scores for cybersecurity intention, we acknowledge the potential influence of social desirability bias. Future research should emphasise multi-method triangulation. This involves moving beyond surveys to integrate objective measures of behaviour, such as behavioural logs (e.g., actual security policy compliance records) or data gathered through field experiments, to validate self-reported intentions against actual security actions. Where objective data is not feasible, researchers should apply advanced statistical

techniques to account for social desirability bias.

Third, longitudinal designs could track behavioural shifts and threat perceptions over time, providing insight into the temporal stability of the relationships we observed. Furthermore, experimental designs could establish causal relationships and test targeted interventions, such as those aimed at reducing rationalisation or leveraging the power of automated security defaults.

Fourth, the dynamic interplay between perceived threat and neutralisation warrants deeper examination. Qualitative methods, such as interviews or focus groups, could illuminate the cognitive processes that make perceived threat a more prominent predictor for passive risk intentions.

Finally, future research could explore potential mediating and moderating factors in the threat-neutralisation relationship. This could include the influence of organisational culture, ethical climate, or security policy framing.

Collectively, these avenues could advance our understanding of how risk perceptions, justifications, and risk types interact to shape cybersecurity decision-making.

7 Conclusion

This study advances understanding of cybersecurity compliance by showing that perceived threat and neutralisation exert distinct effects on employees' active and passive risk-taking behaviours. Comparative analyses demonstrate that these psychological drivers are not uniform: neutralisation is the stronger predictor for active risks, suggesting rationalisation is a key mechanism for deliberate non-compliance, while perceived threat is more prominent in shaping passive risks, where urgency and awareness are crucial. The high frequency of the passive risk-taking despite elevated perceived threat challenges the assumption that merely increasing threat perception is sufficient for compliance, highlighting the need to integrate theories of habit and automaticity into cybersecurity models.

The findings highlight the importance of tailoring interventions to risk type. For active risks, interventions should focus on reducing rationalisation and for passive risks, they must address inaction and convenience-driven routines, often best achieved through automated security defaults and systems designed to disrupt habit. In sum, this research provides organisations with empirical evidence to move beyond one-size-fits-all security campaigns. By differentiating between active and passive risks, organisations can adopt more targeted strategies to reduce human-centric cybersecurity vulnerabilities. Future research should further examine specific threat components, employ diverse methodologies, and explore contextual moderators.

References

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. doi.org/10.1080/0144929X.2020.1856928

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In *Action control: From cognition to behaviour* (pp. 11-39). Heidelberg, Germany: Springer.

Arend, I., Shabtai, A., Idan, T., Keinan, R., & Bereby-Meyer, Y. (2020). Passive- and not active-risk tendencies predict cyber security behavior. *Computers & security*, 101929. doi.org/10.1016/j.cose.2020.101964

Bagozzi, R. P. (2011). Measurement and meaning in information systems and organizational research: Methodological and philosophical foundations. *MIS quarterly*, 261-292. doi.org/10.2307/23044044

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. (2018). Don't even think about it! The effects of antineutralization, informational, and normative communication on information security compliance. *Journal of the Association for Information Systems, 19*(8), 3

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce it policy violation. *Computers & security, 39*, 145-159. doi.org/10.1016/j.cose.2013.05.006

Baron, J., & Ritov, I. (2004). Omission bias, individual differences, and normality. *Organizational behavior and human decision processes, 94*(2), 74-85. doi.org/10.1016/j.obhdp.2004.03.003

Becker, M. H., Drachman, R. H., & Kirscht, J. P. (1974). A new approach to explaining sick-role behavior in low-income populations. *American journal of public health, 64*(3), 205-216.

Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining technology threat avoidance theory. *Communications of the Association for Information Systems, 44*. doi.org/10.17705/1CAIS.04422

Chowdhury, N. H., Adam, M. T., & Teubner, T. (2020). Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures. *Computers & security, 97*, 101931. doi.org/10.1016/j.cose.2020.101963

Cohen, J. (2013). *Statistical power analysis for the behavioral sciences*: Routledge.

DBIR. (2024). 2024 data breach investigations report. Retrieved from https://www.verizon.com/business/resources/T2bb/reports/2024-dbir-data-breach-investigations-report.pdf

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

Field, A. (2024). *Discovering statistics using ibm spss statistics*: Sage publications limited.

Gruber, V., & Schlegelmilch, B. B. (2014). How techniques of neutralization legitimize norm- and attitude-inconsistent consumer behavior. *J. of business ethics, 121*, 29-45. doi.org/10.1007/s10551-013-1667-5

Honeywell. (2024). *Honeywell grad usb threat report 2024*. Retrieved from https://www.honeywell.com/us/en/reports/2024/usb-threat-report/usb-threat-report-download:

Hong, Y., Xu, M., & Furnell, S. (2023). Situational support and information security behavioural intention: A comparative study using conservation of resources theory. *Behaviour & Information Technology*, 1-17. doi.org/10.1080/0144929X.2023.2177825

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

House, D., & Raja, M. (2020). Phishing: Message appraisal and the exploration of fear and self-confidence. *Behaviour & Information Technology, 39*(11), 1204-1224. doi.org/10.1080/0144929X.2019.1657180

Hwang, J., Lee, H., Kim, K., Zo, H., & Ciganek, A. P. (2016). Cyber neutralisation and flaming. *Behaviour & Information Technology, 35*(3), 210-224. doi.org/10.1080/0144929X.2015.1135191

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.

Johnston, A., Di Gangi, P. M., Bélanger, 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*, 103020. doi.org/10.1016/j.cose.2022.103020

Keinan, R., & Bereby-Meyer, Y. (2012). " Leaving it to chance"--passive risk taking in everyday life. *Judgment & Decision Making, 7*(6). doi.org/10.1017/S1930297500003259

Kensington. (2025). *Secure your device, protect your data*. Retrieved from https://www.kensington.com/siteassets/solution-pages/security/2025/secure-your-device-protect-your-data_white_paper_gb-en_final_1745519661.pdf:

Li, Y., Zhang, N., & Siponen, M. (2019). Keeping secure to the end: A long-term perspective to understand employees' consequence-delayed information security violation. *Behaviour & Information Technology, 38*(5), 435-453. doi.org/10.1080/0144929X.2018.1539519

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

Maruna, S., & Copes, H. (2005). What have we learned from five decades of neutralization research? *Crime and justice, 32*, 221-320. doi: http://www.jstor.org/stable/3488361

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS quarterly, 42*(1). doi.org/10.25300/MISQ/2018/13853

Netskcope. (2025). *Cloud and threat report*. Retrieved from https://www.netskope.com/resources/cloud-and-threat-reports/cloud-and-threat-report-2025:

Neves, C., Oliveira, T., Cruz-Jesus, F., & Venkatesh, V. (2025). Extending the unified theory of acceptance and use of technology for sustainable technologies context. *International journal of information management, 80*, 102838. doi.org/10.1016/j.ijinfomgt.2024.102838

NIST. (2024). *The nist cybersecurity framework (csf) 2.0*. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Ogbanufe, O., Crossler, R. E., & Biros, D. (2021). Exploring stewardship: A precursor to voluntary security behaviors. *Computers & security*, 102397. doi.org/10.1016/j.cose.2021.102397

Ogbanufe, O., Crossler, R. E., & Biros, D. (2023). The valued coexistence of protection motivation and stewardship in information security behaviors. *Computers & security, 124*, 102960. doi.org/10.1016/j.cose.2022.102960

Padayachee, K. (2015). An insider threat neutralisation mitigation model predicated on cognitive dissonance (itnmcd). *South African Computer Journal, 56*(1), 50-79. https://hdl.handle.net/10520/EJC173454

Padayachee, K. (2024). An exploration of dark and light triad personality traits towards situational crime prevention and compliant information security behaviour. *Information & Computer Security*. doi.org/10.1108/ICS-04-2023-0069

Prabhu, S., & Dell, P. (2025a). *The nexus between sanctions and neutralization in information security.* Paper presented at the 58th Hawaii International Conference on System Sciences.

Prabhu, S., & Dell, P. (2025b). A structured review of insider cybersecurity behaviour studies. *Information Security Journal: A Global Perspective*, *34*(6) doi.org/10.1080/19393555.2025.2543458

Prabhu, S., Kocsis, D., & Lew, T. Y. (2025). Beyond the direct impact of sanctions and subjective norms in cybersecurity. *Information & Computer Security*. doi.org/10.1108/ICS-04-2025-0148

Prabhu, S., & Thompson, N. (2020). *A unified classification model of insider threats to information security.* Paper presented at the ACIS 2020 Proceedings.

ProofPoint. (2023). *Cybersecurity: The 2023 board perspective*. Retrieved from https://www.proofpoint.com/sites/default/files/white-papers/pfpt-us-wp-board-perspective-report.pdf

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. doi.org/10.1016/j.cose.2018.09.016

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology, 91*(1), 93-114.

Rogers, R. W. (1983). *Cognitive and pshysiological processes in fear appeals and attitude change: A revised theory of protection motivation*. New York.

Samuelson, W., & Zeckhauser, R. (1988). Status quo bias in decision making. *Journal of risk and uncertainty, 1*, 7-59.

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

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American sociological review, 22*(6), 664-670.

TOI. (2025). 19 billion-plus passwords leaked online: Here are the most common ones. *Times of India* Retrieved from https://timesofindia.indiatimes.com/technology/tech-news/19-billion-plus-passwords-leaked-online-here-are-the-most-common-ones/articleshow/120922025.cms?

Tykocinski, O. E., & Pittman, T. S. (1998). The consequences of doing nothing: Inaction inertia as avoidance of anticipated counterfactual regret. *Journal of personality and Social Psychology, 75*(3), 607. doi.org/10.1037/0022-3514.75.3.607

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

Vance, A., Siponen, M. T., & Straub, D. W. (2020). Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. *Information & management*, *57*(4), 103212. doi.org/10.1016/j.im.2019.103212

Vedadi, A., Warkentin, M., & Dennis, A. (2021). Herd behavior in information security decision making. *Information & management*, 103526. doi.org/10.1016/j.im.2021.103526

Verplanken, B., & Aarts, H. (1999). Habit, attitude, and planned behaviour: Is habit an empty construct or an interesting case of goal-directed automaticity? *European review of social psychology, 10*(1), 101-134. doi.org/10.1080/14792779943000035

Wilcoxon, F. (1992). Individual comparisons by ranking methods. In *Breakthroughs in statistics: Methodology and distribution* (pp. 196-202): Springer.

Willison, R., Warkentin, M., & Johnston, A. C. (2018). Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. *Information systems journal, 28*(2), 266-293. doi.org/10.1111/isj.12129

Xin, T., Siponen, M., & Chen, S. (2021). Understanding the inward emotion-focused coping strategies of individual users in response to mobile malware threats. *Behaviour & Information Technology*, 1-25. doi.org/10.1080/0144929X.2021.1954242

Appendix A: Measurement Items

Measurement Item	Adapted from
Perceived Threat (PT)	
I know my organisation could fall victim to a malicious attack if I <add risky behaviour>.	Ifinedo (2012)
My organisation's information and data are vulnerable to security breaches when I <add risky behaviour>.	Ifinedo (2012)
My organisation's data is susceptible to illegal access when I <add risky behaviour>.	Ifinedo (2012)
A successful attack on my organisation's computer as a result of <add risky behaviour> would be damaging.	Ifinedo (2012)
The consequences of an attack on my organisation, when I <add risky behaviour>, would be severe.	Ifinedo (2012)
The consequences of security breaches that occur because of <add risky behaviour> are significant.	Ifinedo (2012)
Neutralisation (NEU)	
It is alright to <add risky behaviour> if no one incurs a loss.	Moody et al. (2018)
It is alright to <add risky behaviour> if there is no negative impact on the organisation.	Self-prepared
It is alright to <add risky behaviour> if no damage is done to the organisation.	Self-prepared
It is alright to <add risky behaviour> if it seems necessary.	Self-prepared
It is alright to <add risky behaviour> when I have to meet deadlines.	Moody et al. (2018)
It is alright to <add risky behaviour> if it seems like there is no other option.	Self-prepared

Behavioural Intentions (BI)	
I am likely to not <add risky behaviour>.	Vedadi et al. (2021)
I intend to not <add risky behaviour>.	Vedadi et al. (2021)
I plan not to <add risky behaviour>.	Vedadi et al. (2021)

Appendix B: Demographic Profile

	B1	B2	B3	B4	Total	as%
Gender						
Male	62	62	63	57	**244**	49.80%
Female	55	65	57	67	**244**	49.80%
Other	1	1	0	0	**2**	0.41%
Prefer not to answer	0	0	0	0	**0**	0%
Work experience						
2 or less	8	7	4	3	**22**	4.49%
3 to 5	17	11	8	9	**45**	9.18%
6 to 8	17	9	9	11	**46**	9.39%
9 to 11	7	10	24	15	**56**	11.43%
12 or more	69	91	75	86	**321**	65.51%

Copyright

doi: https://doi.org/10.3127/ajis.v29.6011