Journal of User Experience

Vol. 21, Issue 3, May 2026 pp. 112–165

Developing User-Centered Mindsets: A Structured Methodology

Dr. Martin Wilson
Deputy Director
North East Cyber Resilience Centre
The Workstation
Paternoster Row
Sheffield
S1 2BX
United Kingdom
martin.wilson@nebrcentre.co.uk

Dr. Sharon McDonald
Lead User Researcher
Government Digital Service
The White Chapel Building
10 Whitechapel High Street
London
E1 8QS
United Kingdom
sharon.mcdonald@dsit.gov.uk

Prof. Alastair Irons
Emeritus Professor of Computer Science
Abertay University
School of Design and Informatics
Kydd Building,
40 Bell Street,
Dundee,
DD1 1HG
United Kingdom
a.d.irons@abertay.ac.uk

Abstract

Mindsets, behavioral archetypes grounded in user beliefs and actions, are increasingly used in user-centered design (UCD) to communicate complex user behaviors. However, the lack of methodological rigor and transparency in the development of mindsets has limited their credibility and broader application. This study presents a structured six-step methodology for creating and validating mindsets from qualitative data, developed in the context of cybersecurity for micro and small businesses. Drawing from established practices and practitioner insights, this method integrates behavioral theory, thematic analysis, and evidence-based segmentation to produce distinct, actionable mindsets. Key steps include applying the MECE (Mutually Exclusive, Collectively Exhaustive) principle to distill qualitative data, identifying behavioral tensions to define the quadrant axes, conducting face-validity checks, and drawing on best practices from the extant persona literature.

Our resulting mindsets were evaluated through an online survey of 20 professionals who are subject matter experts (SMEs) in cybersecurity. Results indicated high perceived validity and usability, with 75-80% of participants finding the mindsets highly representative and highly likely to improve support of micro and small businesses. Feedback highlighted usability strengths alongside areas for refinement, including the importance of making targeted engagement recommendations actionable as well as some concerns about naming conventions. Our findings suggest that this methodology produces mindsets that are empirically grounded, replicable, and practically useful for engagement design. This study contributes a validated, transferable framework for mindset creation that can be applied across domains in which understanding user motivation and behavior is critical.

Keywords

user-centered design (UCD), mindsets, behavioral archetypes, behavioral segmentation, qualitative research, user insight translation

Introduction

Mindsets have been emerging as tools in user-centered design (UCD), which segments users by beliefs and behaviors to support more tailored design solutions. Unlike personas, which have been grounded in academic research, mindsets have largely evolved from industry practice, resulting in limited methodological guidance and validation. Yet, although their flexibility and intuitive appeal have led to widespread adoption across domains, from finance to public services, mindset development processes have remained opaque, often lacking transparency, rigor, and replicability. This paper responds to these gaps by presenting a structured, evidence-informed methodology for creating and validating mindsets, bridging the divide between academic standards and practical utility. Before we outline our methodology in this paper, we present a review of the existing literature, beginning with the rationale and value of segmenting users.

Approaches to Segmentation

User segmentation has involved organizing individuals into archetypes that reflect their distinct needs, behaviors, and motivations. This approach has avoided the inefficiencies of a one-size-fits-all design, leading to more relevant, usable, and effective outcomes (Marsh, 2022). Segmentation has taken multiple forms. Demographic segmentation has highlighted broad user trends that can be useful for tailoring communication to large, diverse audiences or for identifying groups that may face barriers related to age, disability, income, or language (Kotler & Armstrong, 1999). Psychographic or behavioral segmentation has gone deeper, revealing underlying motivations, barriers, and decision-making patterns. This form of segmentation has been particularly valuable when designing targeted interventions, personalizing support pathways, or addressing complex behavior changes (Baum, 2020). Equally important to the approach has been how insights are communicated to those professionals designing the systems and services; this has typically been achieved through UCD communication tools, such as personas, user archetypes, and user profiles, which have translated segmented insights into accessible, actionable formats. A core feature of these UCD communication tools has been their reliance on segmentation to tailor solutions to distinct user needs, behaviors, and motivations; now we turn to a closer examination of these tools.

UCD Communication Tools

UCD communication tools have translated user insights into clear, engaging, and actionable formats, enabling design and development teams to integrate user needs effectively into systems and services (Baxter et al., 2015). Among these tools, personas have been the most widely used for over two decades (Howard, 2015). Other formats, such as user archetypes (broad groupings of users with shared motivations or behaviors) and user profiles (evidence-based descriptions of real or representative users), have also been employed but have remained less common and less developed in practice. Created from qualitative research, personas have been fictional characters made to represent archetypal users, typically segmented by demographics, job roles, goals, and frustrations (Cooper, 1999). Despite their popularity, personas have faced increasing criticism. They have often overemphasized static traits, such as age or occupation (Chapman & Milham, 2006), which can obscure deeper behavioral patterns and motivations essential for effective design (Cooper et al., 2014; Salminen et al., 2018). Their static nature has also made it difficult to reflect the evolving behaviors, contexts, and psychological states of real users (Salminen et al., 2021). In addition, debate has persisted over the optimal number of personas to use: Too few may oversimplify user diversity and exclude key groups, whereas too many may risk overwhelming design teams (Salminen et al., 2022).

What Are Mindsets

In response, mindsets have gained traction in UX and design as a more flexible alternative to personas (for example, Accenture, 2019). Unlike personas, which have often emphasized static demographic traits, mindsets have comprised four behavioral archetypes that segment users according to their beliefs and actions. This has made mindsets more fluid and grounded in real-world decision-making, enabling designers to align systems of support and services with how users actually think and behave (Lino & Bazoli, 2020). Mindsets have also differed from traditional psychographic segmentation by foregrounding contrasting tensions in beliefs and actions rather than descriptive clusters. The four-quadrant structure of a mindset arose from mapping two orthogonal tensions, yielding a model that is methodologically systematic yet

cognitively simple. This balance has provided sufficient diversity to inform design while remaining accessible and actionable for practitioners (Nitafan, 2019). Although some have advocated that mindsets are a replacement for personas, others have argued that the two can be complementary. The choice has depended on the communication need: Mindsets appear well-suited for conveying broad, high-level insights, such as motivational drivers, whereas personas have offered greater precision for detailing specific roles, needs, or contexts (System Concepts, 2023). The preceding review has established the role of mindsets within the broader ecosystem of UCD communication tools and the methodological challenges that accompany them; we now turn to how industry practitioners design and present mindsets in practice.

Practitioner Approaches to Mindset Design

Mindsets have typically been developed from qualitative user data obtained from user interviews, focus groups, diary studies, and surveys (Nitafan, 2019). Their creation has centered on identifying key behavioral tensions, that is, opposing patterns of belief and action, within qualitative data. These tensions can then be mapped along two axes to generate a quadrant-based model that visually represents distinct user mindsets (Figure 1).

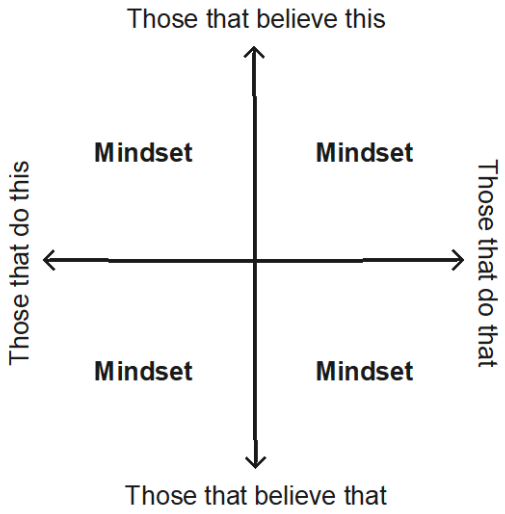

Figure 1: A visualization of opposing beliefs (y-axis) and actions (x-axis) (source: HMRC, adapted from Snart and O'Connor (2022)).

This quadrant visually segmented users into four archetypal groupings, with each grouping representing a distinct way of thinking and acting within a given context. One axis would often capture how users behaved, whereas the other reflected what they believed. This structure has been both diagnostic and generative: It surfaced patterns in current behavior while suggesting tailored strategies for engagement and intervention.

A key strength of the quadrant model used in mindsets has been its fixed axis structure, which segmented all users into one of four behavioral archetypes. Because these mindsets can be defined along continuous axes, users can move between quadrants as their beliefs or behaviors change, whether due to external events, personal experiences, or targeted interventions. This allowed practitioners to both track user transitions over time and design engagements that have helped shift users from suboptimal to more constructive mindsets (Frost & Hendrick, 2020).

Typically, each mindset has been given a memorable name and a bullet-pointed summary of beliefs and actions, deliberately designed to be intuitive, portable, and easy to recall for those using them (Lino & Bazoli, 2020). The accessibility and flexibility of mindsets have made them appealing well beyond traditional software design domains. They have gained particular traction in public services and commercial sectors seeking more nuanced ways to understand user behavior and surface behavioral insights to inform the design of support systems.

Mindsets in Public and Commercial Contexts

Mindsets have been applied in a growing number of public and commercial domains in which motivation and trust have been critical to user decision-making:

- His Majesty's Revenue and Customs (HMRC) developed mindsets to understand how sole traders navigated tax returns, mapping users across dimensions of trust and support needs (Snart & O'Connor, 2022).
- Accenture created financial mindsets to understand banking preferences, based on whether users were rule-following versus instinct-driven and future-oriented versus present-oriented (Accenture, 2019).
- In the military domain, Lanning (2021) used mindsets to support veterans transitioning to civilian life, mapping planning versus reactivity and self-reliance versus external dependence.
- Frost and Hendrick (2020) at the Canadian Digital Service applied mindsets to inform the design of a COVID-19 contact tracing app, segmenting users based on levels of trust in government and their information-seeking behaviors. They developed four distinct COVID-related mindsets using mixed data sources, including user surveys (n = 350), interviews, usability testing, and support requests. However, despite this extensive data collection, their development process remained underspecified, offering limited detail on how behavioral axes were selected, how qualitative data was analyzed, or how the resulting mindsets were validated.

These examples have underscored mindsets' flexibility and usefulness in complex, emotionally charged domains, especially where psychographic segmentation has provided more insight than demographics alone.

However, this growing body of work has largely emerged from practitioner contexts, such as blogs, conference presentations, and applied case studies, in which the emphasis has been typically on why mindsets are valuable rather than how they have been systematically constructed. This likely has reflected the intended purpose of such gray literature, which prioritized accessibility and application over methodological transparency. Consequently, few sources have provided clear, reproducible accounts of how mindsets were derived, validated, or replicated across contexts, leaving their development processes largely opaque and raising concerns about rigor and consistency. The academic literature on mindsets has remained sparse, with most available guidance confined to the gray literature.

Therefore, we next review this material to extract existing methodological insights and assess how mindsets are currently being designed and applied in practice.

Existing Mindset Methodologies

Most literature has emphasized why mindsets are better than personas, but the literature has not explained how to create them. For example, Nielsen (2021) championed mindsets as more dynamic and behaviorally relevant than static personas, yet offered no detail on how to construct them. Similarly, Nitafan (2019) argued for behavioral segmentation over demographic segmentation but provided no practical steps for realizing this shift. Lino and Bazoli (2020) advocated for the integration of mindsets into design activities, but they focused exclusively on application benefits, omitting all methodological detail, such as qualitative data sources or construction processes. A blog by System Concepts (2023) highlighted the potential of mindsets to help teams avoid stereotyping to better meet evolving user needs, but the blog authors acknowledged the lack of clear standards for their development. Even Accenture (2019), in a widely read blog, introduced four financial mindsets without disclosing how they were developed; there was no mention of data, analysis, or validation.

However, two sources have stood out for providing greater methodological transparency. In the following section, we examine these in more detail to explore how their approaches could contribute to a more robust and replicable framework for developing mindsets.

Lanning's Methodology

Lanning began by consulting domain experts with experience supporting Canadian Armed Forces (CAF) members through the transition process. This included personnel from relevant institutions, although the specific individuals or roles involved were not detailed. Secondary research was also conducted to supplement these consultations. However, no further information was provided about the nature of this research, the sources used, or how either the expert input or secondary findings were analyzed.

Learn About Users

These initial consultations and secondary sources appeared to have informed Lanning's early understanding of user experiences and challenges during the transition process. However, the absence of detail regarding data collection methods, participant selection, and analytical procedures limited transparency and made it difficult to assess the robustness or reproducibility of this stage.

Determine Axes

Lanning generated hypothetical proto-mindsets from the secondary data by mapping early assumptions about users' beliefs and behaviors onto two behavioral axes representing opposing traits that were selected to reflect key challenges in the military-to-civilian transition (Figure 2).

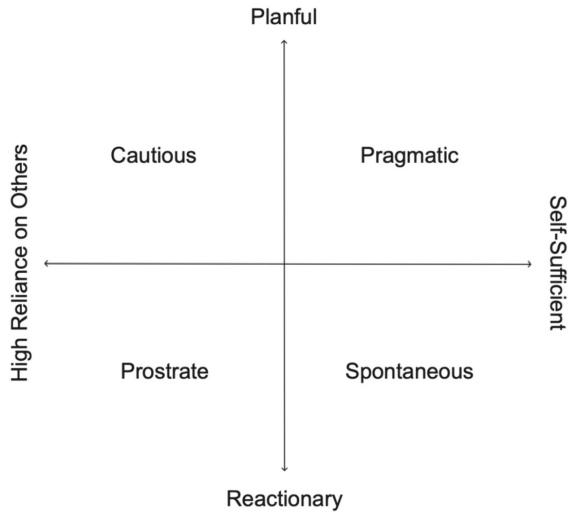

Figure 2: Lanning's (2021) mindset quadrant, mapping four proto-mindsets along two behavioral axes: planful, reactionary, self-sufficient, and high reliance (source: adapted from Lanning (2021)).

Although Lanning noted that other traits (for example, resilience, confidence, and detail orientation) could be used to populate the axes, she stated that choosing the most relevant requires iterative testing and contextual judgment. However, no detail was provided on how this testing or judgment should be applied. Although this approach aligned axes with relevant behavioral tensions that could be used for design, it appeared to be assumption-driven rather than systematically grounded in data, raising concerns about reproducibility and potential researcher bias.

Determine Mindsets

With the axes defined, Lanning's next step was to assign a descriptive name to the mindset in each quadrant (Figure 2). She advised that these names should take the form of an adjective or verb that captures how individuals in that mindset typically approach problems, based on the traits represented by the axes. However, it was unclear whether these labels were grounded in user data or derived solely from the conceptual dimensions of the axes.

Hypothesize Mindsets' Needs, Beliefs, and Behaviors

Lanning used a template provided by the Canadian Digital Service to present her proto-mindsets (Figure 3).

Descriptive Mindset Name	**Three descriptive adjectives** that capture the core essence or tone of the Mindset.	
A value statement articulating what the user prioritizes	A **summary paragraph** outlining the mindset's general outlook, emotional state, and coping approach.	
Key Behaviors A short, bulleted list capturing the user's typical actions or habits	**Beliefs & Attitudes** A few bullet points outlining what the user values, how they think about the situation, and their general outlook or priorities.	**Needs** A clear list of what this user type requires to succeed or feel supported - such as types of information, tools, or guidance. These should reflect what enables or hinders their progress

Figure 3: The template used by Lanning (2021) to structure proto-mindsets, including fields for naming, value articulation, descriptive adjectives, summary narrative, typical behaviors, user beliefs and attitudes, and key support needs (source: adapted from Lanning (2021)).

This structured format added clarity and consistency to how mindsets have been presented. However, the development process appeared to rely primarily on Lanning's interpretation, with limited detail provided on how qualitative data informed the construction of the mindsets. In particular, the absence of explicit procedures, analytical steps, or traceable links between data and outputs made it difficult to assess how systematically the template was populated. As a result, the mindsets may have reflected interpretive insights rather than clearly documented patterns derived from the data.

Consult With Recently Transitioned Veterans

Lanning next developed a set of interview criteria aimed at understanding the experiences of transitioning CAF members. She conducted interviews with six veterans. However, no record of the interviews was provided, which limited transparency and prevented any assessment of the interviews' appropriateness or replicability. According to Lanning, the goal of these conversations was to gain a high-level understanding of each participant's transition journey. These insights were used to inform the development of a custom 3-point rating scale (1, 3, 5) for each behavioral axis, with clearly defined descriptors at each level (Figure 4).

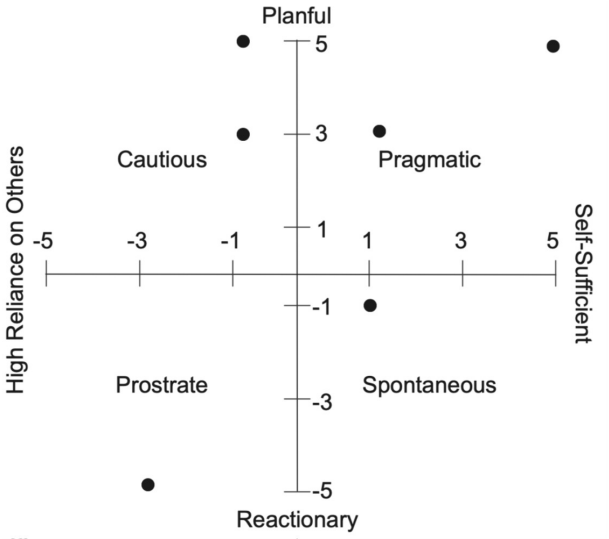

Figure 4: Lanning's (2021) mindsets for Armed Forces Members transitioning to civilian life, plotted along planful, reactionary, reliance, and self-sufficiency axes (source: adapted from Lanning (2021)).

Plot Veterans on a Matrix

Using the rating scales, Lanning assigned scores to individual veterans, allowing them to be plotted within the quadrant model based on their observed behaviors, attitudes, and needs. For instance, on the planful axis, a score of 1 denoted minimal planning and reactive behavior, whereas a 5 represented proactive, well-organized preparation. Similarly, the self-sufficiency axis ranged from high reliance on others (1) to independently managing transition-related tasks (5). Lanning claimed that this scoring system enabled more precise plotting within the quadrant framework, making it possible to distinguish sub-groups within each mindset and tailor support accordingly. Although this method offered greater granularity and user insight, most existing mindset literature has not adopted such precision. Instead, most have relied on a single global placement of a user within a quadrant.

Validate the Mindsets

Once interviewees were plotted on the matrix, Lanning revised the proto-mindsets using the interviewees' input and feedback, which were gathered from stakeholders. However, no detail was given about the specific changes made, how validation was conducted, who the stakeholders were, or how the consultation was carried out, limiting both transparency and reproducibility. Moreover, this approach may have been affected by social desirability bias, in which participants gave responses they believed were expected or acceptable (Larson, 2019). In this context, veterans may have underreported traits associated with less favorable mindsets, which risked distorting the results and weakening the validity of the findings.

Lanning's method was followed by Snart (now publishing as Clayton) and O'Connor's approach.

Clayton (Snart) and O'Connor's Mindset Methodology

Snart and O'Connor (2022) developed four financial mindsets related to sole trader tax returns, publicly sharing their creation process through a slide deck and YouTube™ video presented at the 2022 Service Design in UK Government conference on behalf of HMRC. Their approach began by outlining clear research goals and then collecting qualitative data needed to create mindsets.

User Research and Preparation

Clayton and O'Connor began by defining their user research goal to understand the behaviors, attitudes, and needs of sole traders completing tax returns. To achieve this, they conducted 60 diary studies with sole traders, along with an unspecified number of surveys and interviews. No detail was provided on the sampling, question design, or how the data from these studies were analyzed, limiting the transparency and reproducibility of this stage.

Axes Identification and Segmentation

Clayton and O'Connor stated they had identified key behavioral and attitudinal tensions in their collected data, such as avoid versus embrace tax and path-follower versus pathfinder, which they used to define the axes for four mindsets. However, no detail was provided on how they identified these tensions. Each mindset quadrant was then assigned a descriptive name and caricature designed to intuitively convey the distinct behavioral and actional tendencies of each mindset (Figure 5).

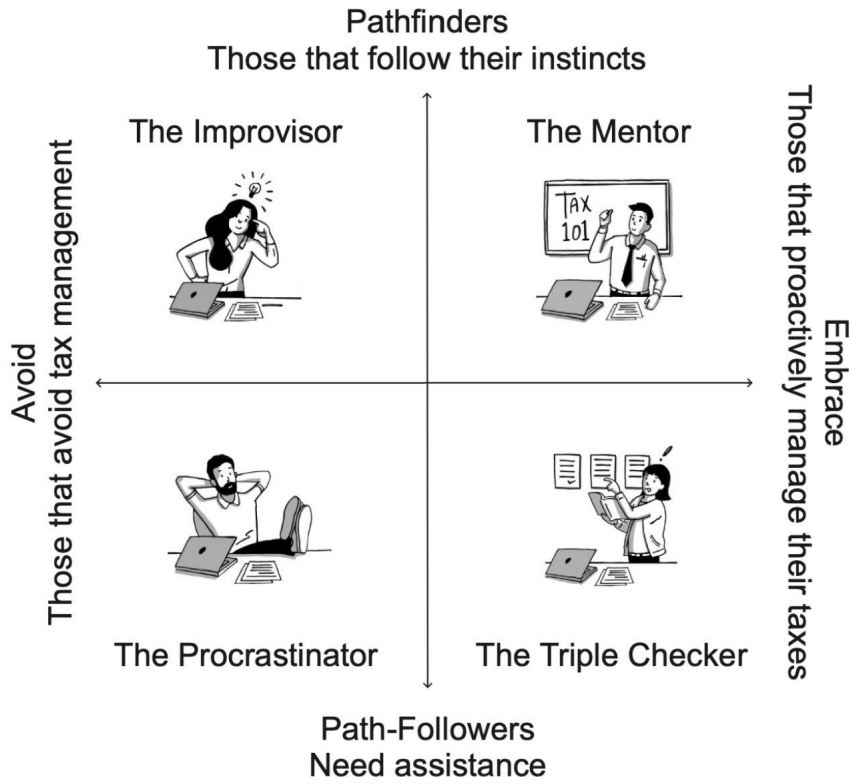

Figure 5: Clayton and O'Connor's four HMRC financial tax-related mindsets, plotted across two behavioral axes: approach to tax (avoid versus embrace) and self-direction (path-follower versus pathfinder) (source: HMRC, adapted from Snart and O'Connor (2022)).

Ensuring Mindsets Are Distinct and Do Not Overlap

In their next step, Clayton and O'Connor applied Minto's (2021) Mutually Exclusive, Collectively Exhaustive (MECE) principle to ensure that each mindset quadrant represented a distinct (non-overlapping) and comprehensive (fully inclusive) set of user behaviors. However, they provided no detail on how this was operationalized, limiting both the transparency and reproducibility of their approach.

Mindset Presentation

Having ensured distinctiveness, Clayton and O'Connor then used a structured format to present their mindsets (Figure 6).

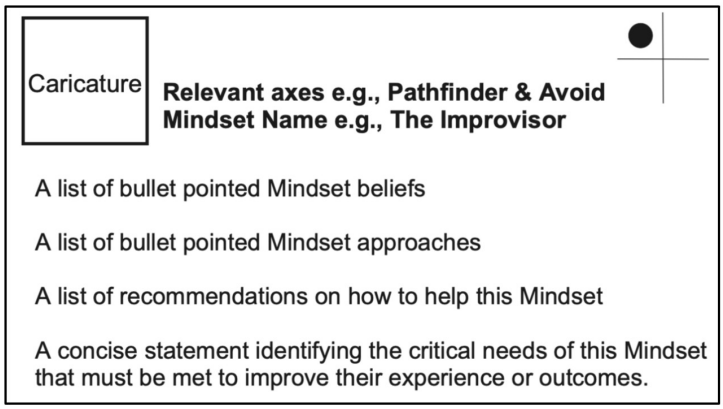

Figure 6: Layout used to present each mindset, including beliefs, approaches, tailored design recommendations, and needs (source: HMRC, adapted from Snart and O'Connor (2022)).

No detail was provided on how many beliefs or approaches were identified overall, or how they were assigned to each mindset. Although three of each were listed per mindset, it was unclear whether additional items were considered or how inclusion decisions were made. For the engagement recommendations, stakeholders with prior experience supporting sole traders were consulted and asked to suggest support strategies. However, there was no detail on who these stakeholders were, how their expertise was established, how their input was matched to specific mindsets, or whether any suggestions were excluded. Crucially, no form of validation was reported once the mindsets were finalized, representing a major methodological omission.

Building on our review of Lanning's work as well as Clayton and O'Connor's approach, the next section summarizes the key methodological gaps that have persisted across the wider mindset literature.

Critical Reflections on Current Mindset Methodologies

The existing mindset literature has consistently emphasized the need to collect qualitative data directly from users, or as appropriate, proxies with close knowledge of the target group, yet it has offered scant guidance on crucial aspects of that collection. The literature has neither recommended a preferred method (interviews, surveys, and focus groups have been cited interchangeably) nor has it explained how to identify the most informative participants, determine a sample size that ensures reliable and representative mindsets, or craft interview questions capable of eliciting the deep behavioral and attitudinal insights required.

We now examine each of these areas in more detail to identify best practices for creating robust and evidence-informed mindsets.

Choosing the Best Data Collection Method

The extant mindset literature suggested that mindsets can be constructed from qualitative user data gathered through interviews, focus groups, diary studies, or open-ended surveys (Nitafan, 2019). This raised a key question: Which of these methods has been best suited to mindset creation? In-depth interviews have been widely regarded as the most effective method for collecting deep behavioral insights, particularly when exploring complex, context-dependent, or sensitive topics (Bowling & Ebrahim, 2005). Interviews have enabled flexible, probing dialogue that uncovers underlying beliefs, motivations, and behaviors (Carter & Henderson, 2005), which have been core components of mindsets. Unlike focus groups, which can reveal group norms but may inhibit personal disclosure due to peer influence (Morgan, 1997), interviews have supported individual, nuanced probing without social pressures. Compared to diary studies,

which have provided a longitudinal perspective but depended heavily on participant compliance while lacking interactive probing (Carter & Henderson, 2005), interviews have allowed real-time adaptation of questions and follow-up on emerging insights. Similarly, whereas open-ended surveys have offered breadth, they typically lacked the depth and flexibility needed to capture rich behavioral reasoning and context (Patton, 2002), further underscoring interviews as the most optimal method for obtaining data to create mindsets.

How to Identify the Right Users

Identifying the right users has been a critical foundation for meaningful mindset development, as mindsets must accurately reflect the beliefs, motivations, and behaviors of the people they are intended to represent (Nielsen, 2021). Engaging participants with relevant lived experience, domain-specific knowledge, or decision-making responsibilities within the target context increased the likelihood of generating the data required to create mindsets. This could be achieved through purposive sampling, a method that involves deliberately selecting individuals who closely align with the target user profile (Bernard, 2017) or by involving proxy participants who possess significant experience working with or observing the target population. This dual approach has been widely used in qualitative research for the identification and selection of information-rich cases related to the phenomenon of interest (Palinkas et al., 2015).

How to Determine a Sufficient Sample Size

The lack of guidance on mindset sample size has represented a significant methodological gap: Too few participants can risk producing mindsets that are unrepresentative or lack sufficient depth, whereas too many can lead to unnecessary data collection, escalating costs, extending timelines, and placing undue strain on research resources. Turning to the extant persona literature, which has shared similarities with mindsets, it suggested that 5-15 interviews per user segment can often be sufficient to identify meaningful patterns (Mulder & Yaar, 2007). Additionally, user research practices such as usability testing have recommended a wave-based approach, in which interviews are conducted in small batches (for example, 5-8), followed by interim analysis to assess whether new themes are still emerging (Nielson, 2012). A practical approach has been to start with approximately 10 interviews per user group, check for saturation, and if new insights still emerge, add incremental batches of 5 interviews until saturation is reached. This has balanced rigor and efficiency, grounding the mindsets in evidence and avoiding unnecessary oversampling.

How to Formulate Questions

The mindset literature has offered limited guidance on how to design interview questions capable of eliciting the nuanced behavioral and attitudinal insights essential for meaningful mindset creation. Poorly constructed questions have risked producing shallow or irrelevant qualitative data, particularly in relation to users' motivations, beliefs, and behaviors, leading to inaccurate, unrepresentative, or incomplete mindsets. Emerging evidence from behavioral science has suggested that theory-informed questions are significantly more effective at eliciting user intentions and attitudes than those lacking a theoretical basis (Tebb et al., 2016). Although Tebb et al. did not recommend a specific model, they emphasized that the choice of theory should be guided by the context of the problem and the characteristics of the target user group. Therefore, our interview questions were grounded in preventative health theory, specifically the Health Belief Model, a framework increasingly applied with success to understand user cybersecurity behaviors (Alsharida et al., 2023).

Having reviewed key considerations for gathering qualitative data, we now present a global overview of the mindset literature in Table 1, which summarizes how each source has performed against six core methodological criteria.

Table 1 presents these findings:

Data: Whether qualitative data collection methods, such as question design, participants, and sample size, were described

Analysis: Whether data analysis procedures used to create mindsets were explained

Axis ID: Whether axis derivation to create mindsets were documented

Traits: Explanation on how mindset traits were identified and assigned to each mindset

Experts: How domain experts were identified, recruited, or used in mindset construction

Validation: Whether any form of mindset validation was described

Table 1: Methodological Transparency in Existing Mindset Literature

Source	Data	Analysis	Axis ID	Traits	Experts	Validation
Accenture (2022)	✗	✗	✗	✗	✗	✗
Frost and Hendrick (2020)	Partial	✓	✗	✗	✗	✗
Lanning (2021)	Partial	Partial	Partial	Partial	Partial	Partial
Lino and Bazoli (2020)	✗	✗	✗	✗	✗	✗
Nielsen (2021)	✗	✗	✗	✗	✗	✗
Nitafan (2019)	✗	✗	✗	✗	✗	✗
Snart and O'Connor (2022)	Partial	Partial	Partial	Partial	Partial	✗
System Concepts (2023)	✗	✗	✗	✗	✗	✗

✓ = Fully described, ✗ = Not described, Partial = Mentioned without sufficient detail

In summary, the current mindset methods literature has remained underdeveloped. Most offered conceptual strengths but lacked the rigor needed for replicability. This paper responds to these limitations by building upon the methodologies presented by Lanning as well as Clayton and O'Connor to offer a structured, research-informed method that is both academically robust and practically usable.

Methods

In our method, we applied mindsets in a non-traditional UX domain by communicating the cybersecurity needs of small businesses to small-business cybersecurity consultants. The aim was to help consultants better understand small businesses' diverse cybersecurity perspectives and tailor their engagement and support accordingly. This domain has been marked by persistent engagement challenges, particularly the use of generic one-size-fits-all approaches that overlook the varied needs of different small business user groups (Wilson & McDonald, 2024). The UCD-based mindset approach offered a promising path to address this by segmenting small businesses into four distinct mindsets based on their cybersecurity beliefs and behaviors, enabling more targeted, relevant, and effective support. However, our aim was not to present insights into the small-business cybersecurity domain, but rather to use it as a lens to illustrate a clear, transparent, and replicable mindset-creation process that can be adopted and applied across domains.

Methodology Overview

Our approach, presented in this paper, comprised two interconnected phases that produced mindsets, followed by a separate evaluation phase that assessed the mindsets that we generated.

Phase 1: Qualitative Data Collection

In Phase 1, we performed qualitative data collection through

- recruitment of small-business owners and cybersecurity consultants,
- design of interview questions and protocols, and
- thematic analysis of interview data, forming the basis for mindset construction.

For phase 1 materials, we used Microsoft® Teams™ for participant interviews, Qualtrics™ for participant screening, and ATLAS.ti for qualitative analysis.

Phase 2: Mindset Creation

In Phase 2, we created mindsets through

- a six-step derivation of prototype small-business mindsets created from thematic interview data gathered in Phase 1, and
- face-validity checks to confirm each mindset plausibly represented real-world small businesses.

For phase 2 materials, we used Miro™, an online collaborative whiteboard, to cluster thematic data and translate it into each mindset's behavioral tension pairs.

Survey-Based Evaluation

We evaluated the mindsets through

- design and deployment of an online survey for cybersecurity consultants, and
- an assessment by those consultants of each mindset, including the following:
    - Perceived usability: The mindsets' potential to help professionals engage small businesses in cybersecurity
    - Perceived validity: How accurately the consultants perceived the mindsets, which represented the wider small business population

For survey materials, we used a Qualtrics survey so consultants could provide anonymous mindset feedback.

Phase 1: Participants and Recruitment

In Phase 1, we recruited 30 participants and divided them into three distinct groups of 10 individuals. We defined the group categories according to the EU's Small Business Standards Group (SBS, 2020).

Table 2: Classification of DD, DB, and DE Groups

Group Name	**Description**
Digitally dependent (DD)	Businesses that relied on IT/software for operations, but tech was not their core offering
Digitally based (DB)	Businesses whose core products/services were delivered through or built on software/IT, excluding cybersecurity services
Digital enablers (DE)	Cybersecurity consultants who helped other businesses to improve cyber resilience

We facilitated the interview recruitment through the UK Cyber Resilience Centre (CRC) network, adopting a purposive sampling strategy (Barnard, 2017) that targeted small businesses registered with the CRC network that were likely to fit into the DD and DB categories. We directly contacted prospective participants via email. Those who responded to the email were then screened to confirm their alignment with the SBS categories. We conducted the screening with a short online survey that collected demographic and IT usage data and obtained digital

consent. Upon completing the survey, eligible participants were scheduled for interviews. Digital enablers were recruited through the CRC network's cyber-experts panels, who were invited to participate in interviews via email. As it was the digital enablers' experience of supporting small businesses with cybersecurity, no screener survey capturing their Information and Communication Technology (ICT) use was required.

Interview and Question Design

To ground our interview design, we drew on the Health Belief Model (HBM) (Rosenstock et al., 1988). HBM posited that action is driven by six belief-based constructs: susceptibility, severity, benefits, barriers, cues to action, and self-efficacy. These have shaped behavioral intention, a strong predictor of whether people adopt protective measures. Our interview questions were aligned with each HBM construct and informed by prior cybersecurity research using the model to explore why small businesses choose to invest, or not invest, in cybersecurity.

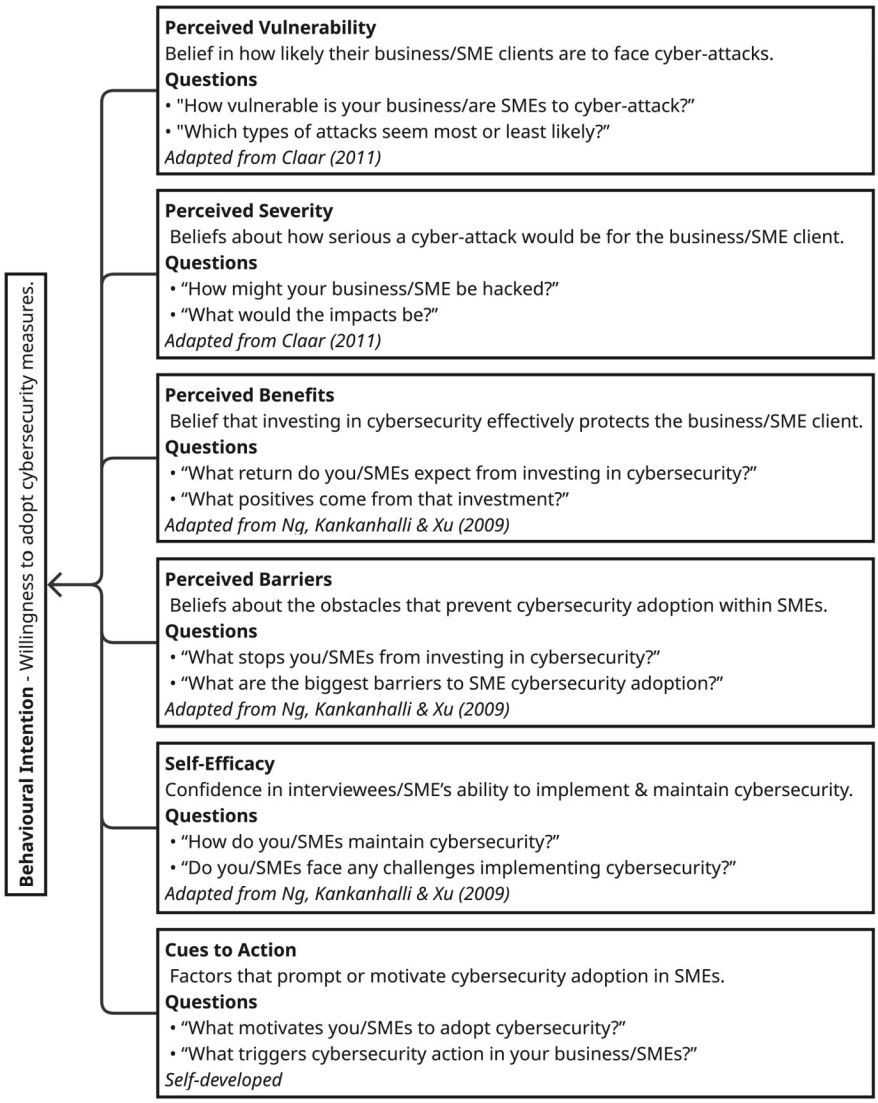

Figure 7: The interview question framework mapped to the HBM constructs, illustrating how each psychological factor was explored to understand small-business cybersecurity behavior. Questions were adapted from existing research or self-developed by the authors.

In addition to the HBM-aligned questions, we also developed a small set of exploratory questions to gather deeper insights into these questions:

1. How are digital enablers (DE) engaging subject matter experts (SMEs) on cybersecurity?
2. How are digitally dependent (DD) and digitally based (DB) businesses seeking cybersecurity guidance?
3. What is the influence of media reporting on perceptions of cyber risk?
4. What are ideas for improving small business cybersecurity in the future?

These exploratory questions are summarized in Table 3.

Table 1: Self-Developed Interview Questions

Group(s)	**Topic Area**	**Questions**
DE	SME engagement	What do SMEs ask you for help with regarding cybersecurity? How do you contact SMEs to discuss cybersecurity? What works best when persuading them of cybersecurity's importance?
DD, DB	Guidance seeking	Have you heard of the National Cybersecurity Centre (NCSC)? How do you currently receive cybersecurity guidance? How would you like to receive cybersecurity guidance?
DD, DB	Media influence	How do media reports of cyber-attacks influence your security adoption? In what ways, if any, do these news stories resemble your business context?
DD, DB, DE	Future improvements	What can be done to improve the future of SME cybersecurity?

All questions were piloted with cybersecurity professionals, business owners, and academics to ensure clarity, technical accuracy, and freedom from bias. Before participating, all individuals were provided with a combined information sheet and consent form outlining the study's aims, procedures, and their rights; no incentives or compensation were offered.

Conducting and Transcribing Interviews

We conducted online interviews using Microsoft Teams video conferencing. Teams software allowed the recording and automatic transcription of the interviews. These transcriptions served as initial drafts and underwent rigorous verification to ensure accuracy. Any identifiers were removed from the transcripts, and each interviewee was assigned a relevant pseudonym.

Data Analysis

We analyzed interview transcripts inductively in Atlas.ti 23, developing codes iteratively and consolidating them into a structured codebook containing 12 themes and 1,530 quotations. To assess consistency, the second author independently coded 25% of the transcripts using the codebook; intercoder reliability, calculated with Krippendorff's α, was 0.73, indicating substantial agreement (Landis & Koch, 1977).

Phase 2: Mindset Creation

The aim of this methodology was to offer a clear, six-step process for creating and validating mindsets. It integrated the strongest elements of Lanning's as well as Clayton and O'Connor's approaches while filling their gaps, clarifying ambiguous steps, and addressing limitations. We started by applying the MECE principle to the thematic interview data from Phase 1.

Step 1: Applying the MECE Principle

The MECE principle distilled voluminous qualitative data into a more manageable data set by following two complementary rules:

- Mutually Exclusive: Each data point is placed in one, and only one, category, eliminating overlap and redundancy.
- Collectively Exhaustive: All meaningful data is represented; no relevant insight is left out.

The benefit of using the MECE process in mindset creation was that it made latent patterns easier to see, enabling us to identify behavior-action pairs within the data that would become our mindset's X and Y axes.

To begin, we refined the Phase 1 thematic dataset by removing quotations not directly related to micro and small-business cybersecurity behaviors—specifically those focused on the engagement tactics used by digital enablers to promote cybersecurity. These were set aside for separate analysis, leaving 1,325 behavior-focused quotations.

To make this 1,325-quotation data set more manageable, each quotation was placed into a digital Miro note (similar to a Post-it note) in a Miro board. Short quotations were copied directly, whereas longer ones containing full sentences or phrases were replaced with concise, descriptive sentences or labels that captured the parent quotations' core meaning. This ensured the dataset was collectively exhaustive, with every quotation represented for further analysis.

Next, to achieve mutual exclusivity, we reviewed the Miro board to identify and remove duplicate Post-it notes expressing the same underlying meaning. For example, three Post-it notes labeled "phishing," "email-based threats," and "spear phishing" were consolidated into a single Post-it titled "phishing." This process ensured each behavioral insight was represented only once, resulting in a refined dataset of 98 unique and distinct quotations, each displayed on an individual Post-it note (Figure 8).

Tip: Always cross-check any ambiguous Post-it note label against the original interviewee quotation to ensure the meaning was preserved. Adjust the wording if the condensed label risks oversimplifying or misrepresenting the original meaning.

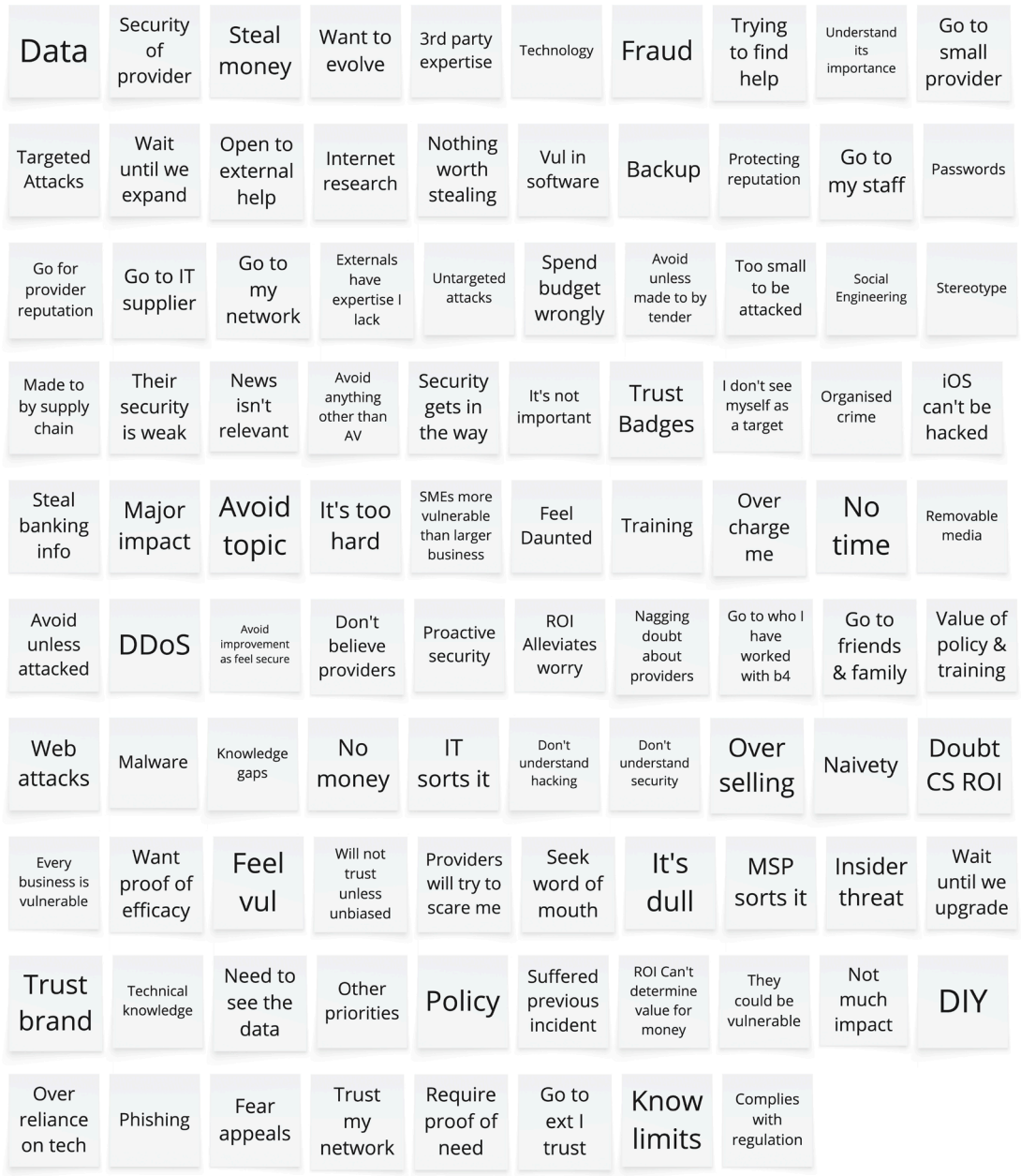

Figure 8: Miro board containing the 98 condensed quotations representing interviewee cybersecurity attitudes and behaviors.

Step 2: Identify Core Behavioral Tensions (Mindset Axes)

The aim of step 2 was to identify one pair of opposing beliefs and one pair of opposing actions to serve as the mindset framework's X and Y axes. This was a critical step as these tensions anchored the entire framework; misidentifying them would undermine the mindset's validity. To identify tensions, we conducted an evidence safari whereby researchers virtually collaborated using a shared Miro board to surface the two axes that defined our mindset framework from the 98 Post-it notes. This was an iterative process involving passes, or sweeps, through the data to surface the axes.

PREPARE THE BOARD

We imported every quotation (98) as a separate Post-it on a shared Miro board, and we titled the board with two workspace lanes for beliefs and actions.

In pass 1, we grouped the Post-it notes by

- placing each Post-it into its correct lane (what interviewees thought versus what they did),
- within each lane, grouping notes together that expressed the same or very similar idea or meaning, and
- giving every group a short, descriptive label that collectively encapsulated the Post-it notes within.

Our outcome was approximately 12 small, clearly named groups (Figure 9).

Tip: To distinguish between belief and action quotations, ask yourself this: "Is this what the interviewee thinks or feels (a belief), or is it something they say they do or would do (an action)?" If the meaning isn't immediately clear, re-read the uncondensed parent quote and consider what is being implied, a thought or behavior, before assigning it as an action or belief.

Figure 9: Miro board containing Post-it notes grouped into action and belief lanes, clustered by theme.

In pass 2, we merged initially identified clusters into broader clusters:

- We reviewed the clusters and identified opportunities to merge them into broader parent clusters that captured a higher level, more abstract meaning. We relabeled them as appropriate at the higher level of abstraction (for example, notes under procrastination from Figure 9 were merged into the cluster for avoid doing cybersecurity, as these notes related to reasons why interviewees said they didn't adopt cybersecurity).

Our outcome was fewer, broader clusters, making it easier to identify high-level beliefs and actions.

Tip: Try to keep belief and action clusters separate through this process.

In pass 3, we surfaced belief and action contrasts by

- continuing to look for merging opportunities of clusters, and
- at the same time, looking for belief and action clusters that were direct opposites of one another (for example, "avoiding cybersecurity" versus "embracing cybersecurity" was an action, but "worried about cyber-attacks" versus "not worried about cyber-attacks" was a belief).

Our outcome showed visible tensions with fewer clusters on the shared Miro board (Figure 10).

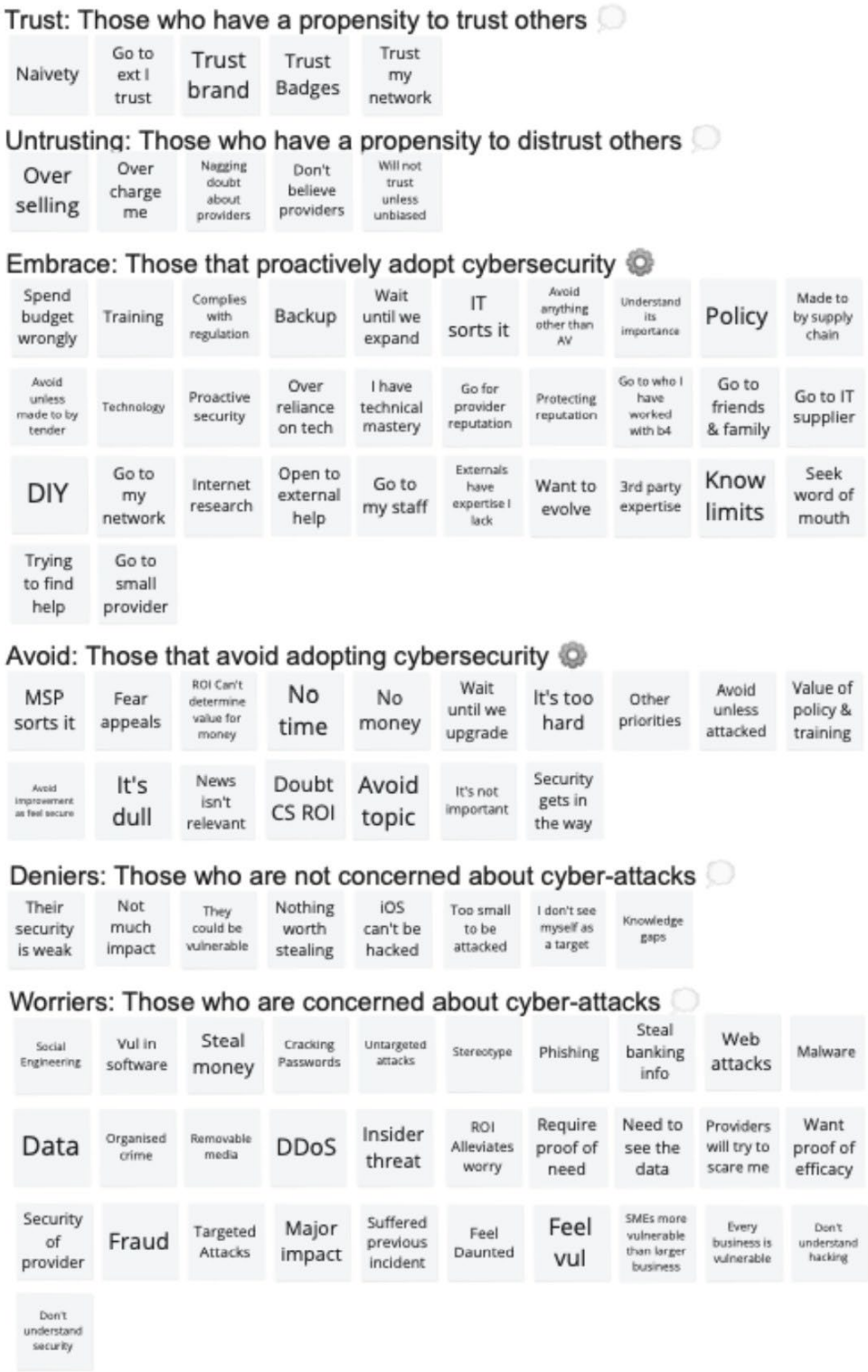

Figure 10: Miro board showing merged clusters from Figure A, now grouped by opposing meanings to surface contrasting beliefs and actions.

In pass 4, we surfaced axes:

- We continued merging clusters until only one pair of opposing belief and action groups remained.
    - In our case, this was:
        - Belief: worriers (concerned about cybersecurity) versus deniers (unconcerned about cybersecurity)
        - Action: embrace (adopt cybersecurity) versus avoid (don't adopt cybersecurity)
    - To achieve these final dimensions, we merged Post-it notes for trust into the adopt group. When we revisited the original quotations, participants described how, once they established trust, they acted. Naivety was also included as a label, as it implied taking action after trusting in the wrong advice. Conversely, Post-it notes for untrust were aligned with avoidance, capturing how a lack of trust inhibited action. We also relabeled cyber-attacks to cybersecurity in the worriers and deniers group descriptions to reflect the higher level of abstraction that the notes collectively represented.
- We conducted one final pass of MECE, ensuring every Post-it appeared once (no overlap) and that no Post-it note was left out.

Our outcome was precisely two pairs of opposing super-groups that were appropriately labeled; the names of which formed our mindset X-Y axes (Figure 11).

Figure 11: Miro board showing final clusters, with color-coded Post-it notes.

Key:

Actions: Green—cybersecurity actions (adopt); red—cybersecurity inaction or avoidance (avoid)

Beliefs: Blue—low concern or dismissive beliefs (deniers); orange—high concern or risk-aware beliefs (worriers)

Mapping these belief and action group descriptive labels onto X and Y axes provided a clear structure for generating our four distinct mindset quadrants (Figure 12).

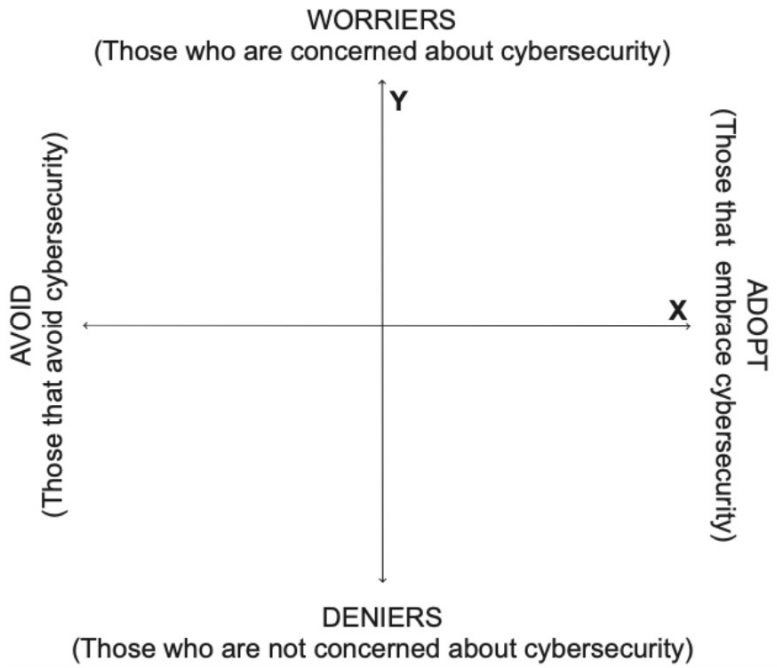

Figure 12: Cybersecurity beliefs and actions group labels mapped on X (adopt-avoid) and Y (concerned-unconcerned) axes to define four distinct mindset quadrants.

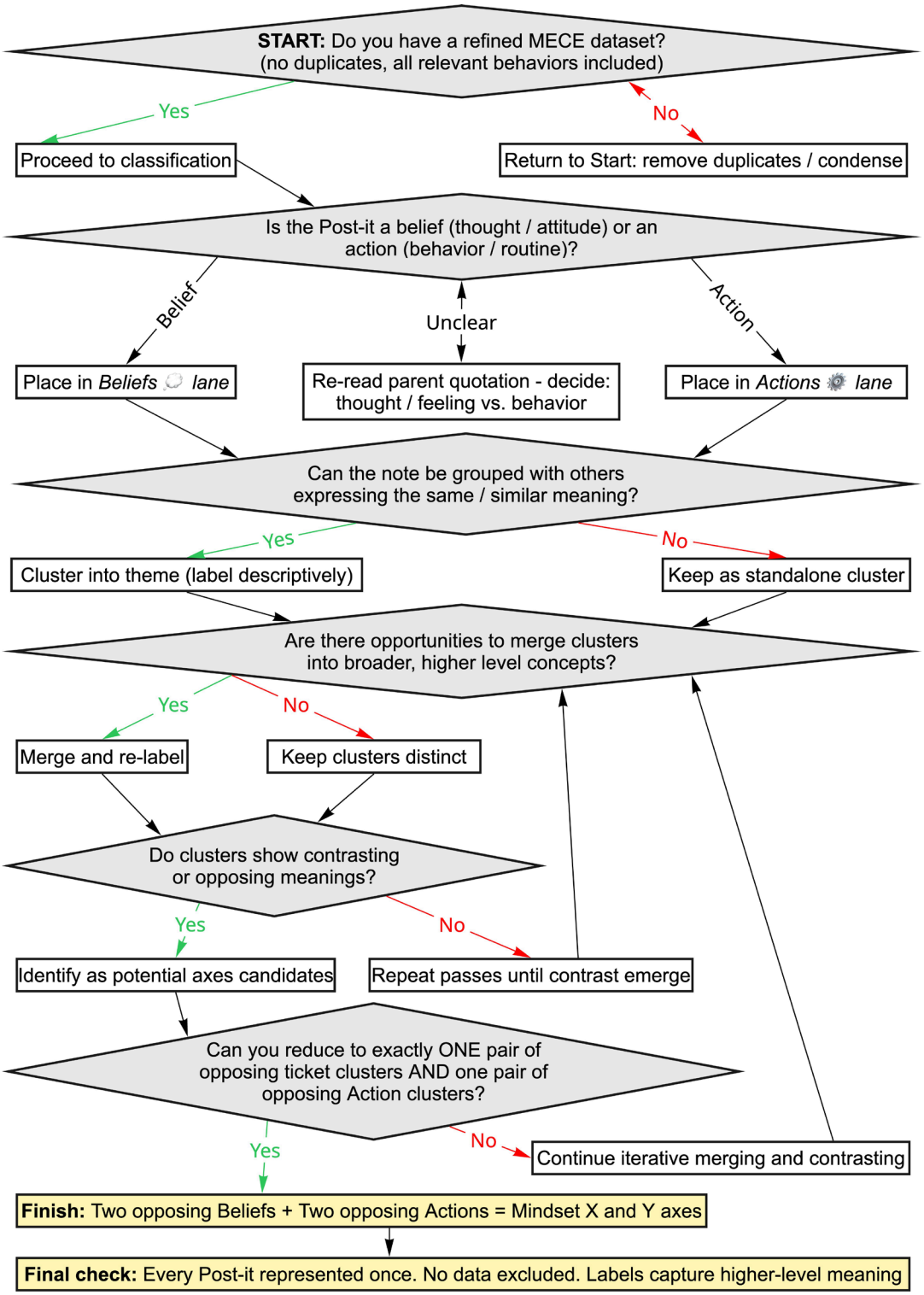

Figure 13. Decision tree outlining the six-step criteria for clustering qualitative data into beliefs and actions, merging and contrasting clusters, and deriving opposing pairs to define the mindset axes.

Step 3: Populating Mindset Quadrants

Once we established our axes, we used them to help position the color-coded Post-it notes within one half of the X-Y mindset framework (Figure 14).

For example:

- Post-it notes related to embrace (green) were placed in the right half only (quadrants B and D).
- Post-it notes related to avoid (red) were placed in the left half only (quadrants A and C).
- Post-it notes related to denial (blue) were placed in the bottom half only (quadrants C and D).
- Post-it notes related to worry (orange) were placed in the top half only (quadrants A and B).

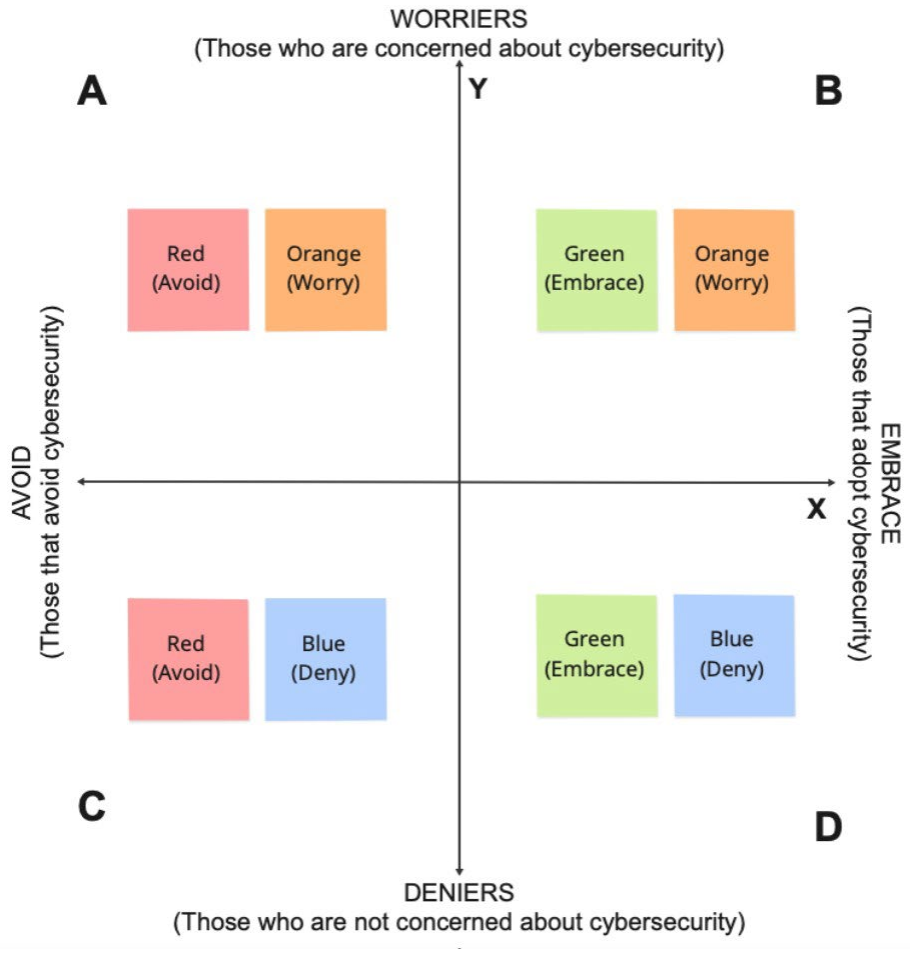

Figure 14: Rules for Post-it placement within one axis half, showing how red notes can only be applied to the left (A and C), blue to the bottom (C and D), green to the right (B and D), and orange to the top (A and B).

Once a Post-it note had been assigned to one half of the mindset framework, the next consideration was to determine its final quadrant, narrowing it down from two possibilities to one.

Final placement was guided by the following sub-steps:

1. Revisiting the original quote: When needed, we referred back to the source quotation. The full context could often reveal nuance that may have been lost in a condensed Post-it label, helping placement decisions.
1. Consulting the literature: Prior findings suggested which mindset quadrant a quote aligned with.
2. Sense checking with experts: Domain knowledge helped. In our case, the first author's decade of experience in SME cybersecurity consultation supported some final placement decisions.
3. Recording the rationale: We noted a brief justification for each decision. These notes helped maintain consistency, supported transparency, and offered a point of reference in the event of a challenge or questions about why notes had been located in certain quadrants.

Figure 15 shows the final placement of Post-it notes within our mindset framework. Although it is not feasible to document every individual Post-it placement decision within this paper, Table 4 provides a sample of some of our decisions and rationale. These examples illustrate how we used a combination of quotations from the original interview context, relevant literature, and domain expertise to make final placements.

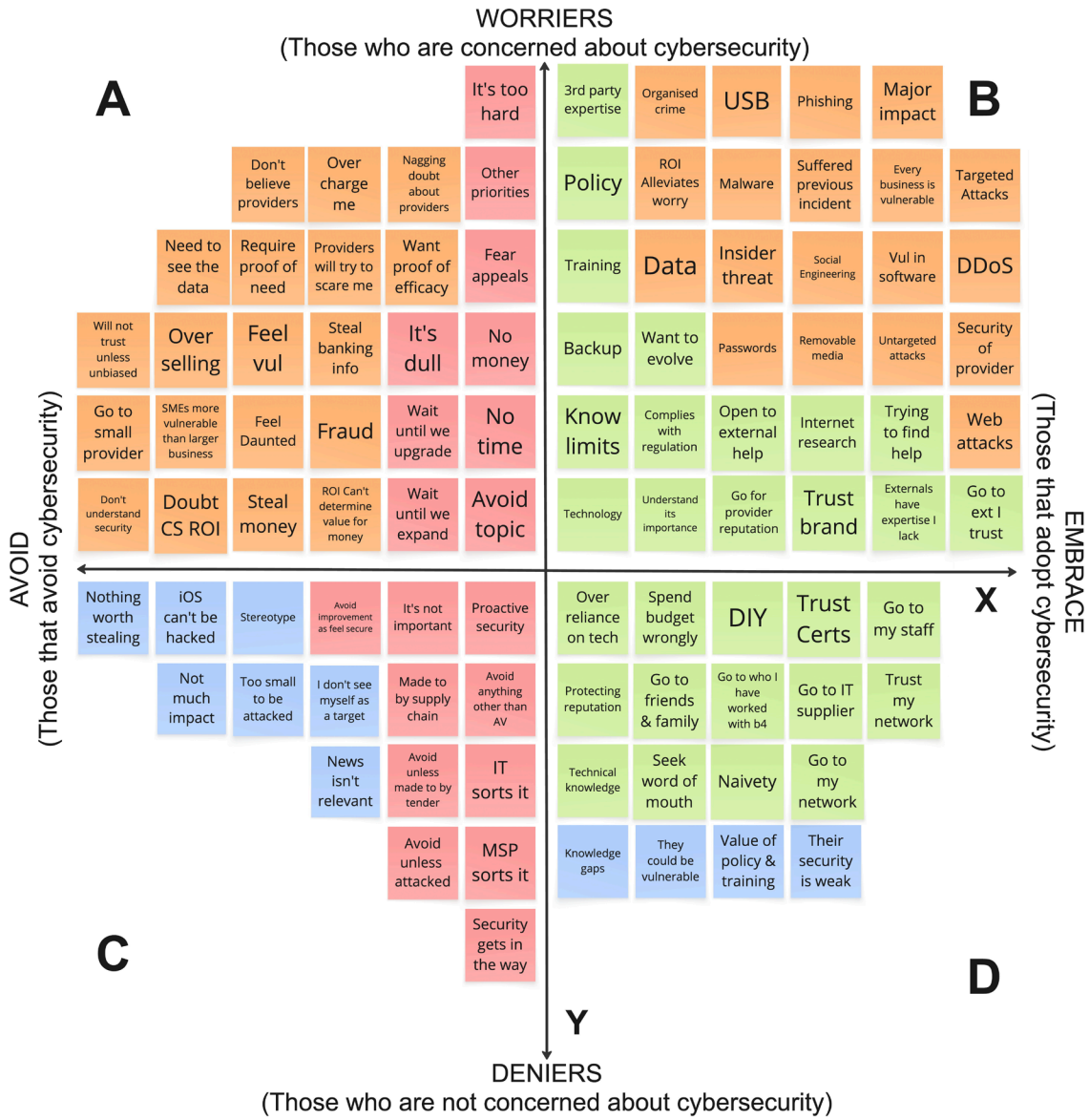

Figure 15: Diagram showing placement of Post-it notes into final mindset quadrants.

Key: Green = adopt, red = avoid, blue = not concerned, orange = concerned

Table 4: Example Rationales of How Selected Post-It Notes Were Assigned to Final Mindset Quadrants

Post-It Summary	Initial Half	Diagnostic Clues	Final Quadrant
Feel Daunted 🟠 – "I know cyber is important, but it's very intimidating."	A or B	**Worried** about cybersecurity, but overwhelm leads to **inaction**. Supported by the first author's experience with small businesses expressing similar concerns.	A
IT sorts it 🔴 – "I'm not that concerned about cyber as my IT supplier sorts it."	A or C	**Not worried**; delegates responsibility to a trusted IT provider, resulting in **inaction**. Supported by Wilson et al. (2022), who found similar confidence in outsourced IT among small businesses.	C
Their security is weak 🔵 – "I have lots of techie engineers that really know this stuff and do security for me."	B or D	Overconfident (**denial**) in internal expertise; believes **action already taken** is sufficient. Supported by Wilson and McDonald's (2024), based on interviews with consultants concerned about small businesses' overconfidence.	D
Know limits 🟢 – "I'm good with IT, but I know that cyber's different and I have my limits."	B or D	Recognizes the importance of cybersecurity, **takes action**, and values external input. Confirmed by revisiting the original interview quote.	B

Key:

Post-it summary: A condensed version of an original interviewee quote was used during Miro board clustering, including (🟢) embrace, (🔴) avoid, (🔵) denial, and (🟠) worry.

Icons indicated whether the Post-it represented an action (🟢/🔴) or a belief (🔵/🟠) as described by the interviewee.

Initial half: The two possible quadrants the note could initially belong to were based on its belief (Y axis) and action (X axis).

Diagnostic clues: Justification was recorded for final quadrant placement. Bold indicated the relevant mindset axis (belief or action).

Final quadrant: The specific mindset quadrant (A, B, C, or D) was recorded for the notes' ultimate placement.

With each quadrant populated, we then interpreted the shared meaning of its Post-it notes and axis pairing to develop four distinct mindsets, each defined by a descriptive name, illustrative caricature, and a summary of typical cybersecurity beliefs and behaviors.

Step 4: Bringing Quadrants to Life

Once every Post-it was placed in its final quadrant, we treated each quadrant as its own self-contained story made up of all the beliefs and actions pinned there. We re-read those notes aloud, asking two questions:

- Dominant motive: Why do businesses in this quadrant think or act this way?
- Dominant pattern: What cybersecurity actions do they typically do (or avoid doing)?

Where those two threads crossed, a recognizable character emerged. We turned each motive and behavior pair into an archetype so anyone—a designer, policymaker, or SME adviser—could grasp it at a glance (Table 5).

Table 5: Translating Cybersecurity Beliefs and Behaviors Into Intuitive/Descriptive Mindset Names

Belief	**Action**	**Mindset Name**
Worried	Inaction	The Procrastinator
Worried	Action	The Pragmatist
Unconcerned	Inaction	The Rationalizer
Unconcerned	Action	The Know-It-All

With the four quadrant names in place, we fleshed out each archetype by adding a concise description, key beliefs, and typical behaviors. We performed the following:

1. Gathering the strongest evidence:
    - We pulled 5–7 Post-it notes that best represented the quadrant's cybersecurity voice.
    - We converted them into two bullet lists for common beliefs and typical approaches, each illustrated with a short verbatim quote from Phase 1 to enhance emotional depth and contextual richness.
2. Adding a visual cue:
    - We matched every archetype with a simple caricature that instantly conveyed its mindset, making the profiles memorable and intuitive.
3. Crafting a one-sentence summary:
    - We distilled the mindset's overarching attitude and behavior into a single sentence that gave readers an instant feeling for the archetype they were dealing with.

Figure 16 shows an example of how these elements combined to create a complete mindset profile.

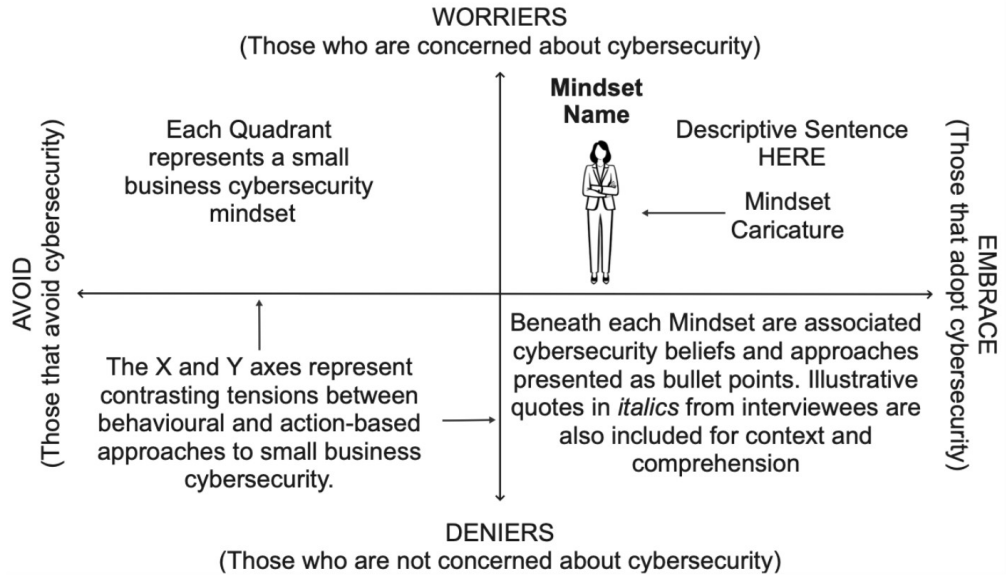

Figure 16: Mindset construction.

With mindset names, caricatures, beliefs, and typical behaviors defined, the next step was to develop tailored engagement recommendations, that is, practical strategies designed to address the specific needs, concerns, and tendencies of each mindset.

Step 5: Designing Engagement Recommendations

Following the precedent set by Clayton and O'Connor's mindset framework, we included a tailored "How to Help" section for each mindset. These numbered recommendations were customized to reflect the distinct cybersecurity beliefs, behaviors, and barriers associated with each archetype, ensuring that engagement advice was both targeted and actionable.

To do this, we revisited the 205 digital enabler quotations we had set aside during step 1. Using the MECE principle, we grouped and refined these quotes into discrete, standalone engagement tactics, ensuring there was no overlap or omission. This process allowed us to compile a list of recommendations, from which we could map to the most relevant mindset quadrant using the first author's expert domain judgment or a reference to the literature:

1. Domain judgment: The first author's decade of advising small businesses on cyber risk informed certain choices
2. Literature cross-check: Research that suggested the tactic is effective for businesses with comparable beliefs or barriers informed certain choices

Table 6 presents four worked examples (one for each mindset) to illustrate this mapping process. Our sample showed how distilled digital-enabler tactics were assigned to the most appropriate mindset by combining domain judgment with the supporting literature.

Table 6: Four Illustrative Matches

Mindset	**Assigned Tactic**	**Tactics' Relevance**	**Judgment or Literature**
Rationalizer	Use live-hacking demos to expose the random nature of attacks and how easily basic cyber defenses can be exploited	Visually disproves the idea that "only big targets get hacked," replacing the nothing-worth-stealing belief with increased risk awareness	Small-business cybersecurity research (Wilson et al., 2022)
Procrastinator	Break larger security tasks into micro-goals with explicit deadlines	Micro-goals reduce overwhelm and trigger action, an antidote to anxious avoidance	Procrastination research on implementation intentions (Steel, 2010)
Pragmatist	Provide a gap-analysis and roadmap that aligns with best practice	Pragmatists crave structured, evidence-based progress; a roadmap lets them benchmark and iterate	Repeated finding in SME consulting (first author's 10 years field work)
Know It All	Point to authoritative guidance (Gov), stressing policy, training, and layered controls	De-personalizes advice and appeals to their respect for recognized expertise, sidestepping "I already know that" pushback	Repeated finding in SME consulting (first author's 10 years field work)

Using this same judgment and literature approach, every remaining tactic was routed to one or occasionally two mindsets as appropriate, resulting in mindset-specific recommendation bullet points that practitioners can use.

Tip: If you didn't interview domain experts during your initial research (as we did in Phase 1), you may not have a ready-made set of engagement tactics to draw from. In that case, consider involving relevant experts at this stage. Ask them what approaches they would recommend for addressing the needs, beliefs, and behaviors of each mindset.

Step 6: Face Validity Checks

The final step in our mindset creation was to assess the validity of our mindsets. To do this, we drew on established persona validation strategies from the literature and adapted them to suit the mindset context. In particular, we followed the approach outlined by Huynh et al. (2021), who validated personas by comparing them against the raw qualitative data used to generate them to ask these questions:

- Are our created personas realistic?
- Do they reflect the behaviors and attitudes observed in our data?

We applied these same guiding questions to our mindsets:

- Are the mindsets realistic?
- Do they accurately reflect the attitudes and behaviors observed in the underlying data?

This validation step ensured that each mindset stayed firmly rooted in the original data and accurately reflected the beliefs and behaviors observed in the evidence.

Tip: If a mindset fails the face-validity check, revisit the original quotes to identify what was misinterpreted or overlooked, then revise the name, summary, and bullet points to better reflect the data.

This concluded the six-step process for creating our mindsets.

Figure 17 summarizes the process and includes qualitative data collection guidelines; the mindsets themselves are presented in the Results section. It's worth noting that during the creation process, our priority was to make each mindset conceptually distinct and ensure the full spectrum of user perspectives was captured, rather than quantifying how many interviewees fit into each mindset within our Phase 1 data.

Figure 17: Diagram illustrating the methodological process used to develop the mindset prototypes with the qualitative data collection guidelines.

Next, we outline the method used to conduct an evaluation survey with 20 SME cybersecurity professionals to assess the mindsets we created.

This evaluation was not part of our core mindset creation method, and it does not need to be replicated to create mindsets; rather, it offered deeper insight into whether the resulting mindsets genuinely reflected real-world cybersecurity attitudes and behaviors. If they do, this would strengthen confidence that the method can produce valid, practical mindsets in other domains.

Evaluation Survey Methods

Before outlining the procedure used to develop the survey, we first describe the study design, participants, and materials used.

Study Design

We conducted an anonymous online survey to evaluate the perceived utility and validity of the mindsets by gathering feedback from small-business cybersecurity consultants. We chose a cross-sectional time horizon for the survey due to practical constraints such as participant availability. Although we considered longitudinal studies tracking consultants who use the mindsets with small-business clients, they were ultimately excluded due to concerns about scalability, generalizability, and overall feasibility.

Participants

Twenty participants were recruited via purposive sampling (Bernard, 2017), targeting individuals with direct experience supporting small businesses in cybersecurity. Recruitment was conducted through the first author's professional connections with the UK Cyber Resilience Centre (CRC) and the Police Cyber Protect Network. Although this approach may have introduced bias due to prior professional relationships, it was selected pragmatically as previous studies highlight the difficulty of recruiting such cybersecurity professionals who were not already known to researchers (Osborn & Simpson, 2017); attempts at random recruitment have often failed to yield sufficient participants (Khan et al., 2025). To help mitigate this potential social desirability bias, the survey was anonymous to encourage candid feedback, and our participant sample was divided into two comparison groups:

- CSC group: Independent cybersecurity consultants with no prior connection to the authors
- CRC group: CRC staff and police officers with established professional ties to the first author

This grouping enabled statistical comparison to detect potential bias. No significant differences were found between the two groups in their evaluations, suggesting broadly consistent perceptions of the mindsets across participant types. Although the sample size was modest, it was appropriate given the participants' specialist expertise and the practical constraints of time and availability.

Materials

- The Qualtrics survey platform was used to deploy and collect data for the survey.
- SPSS™ (Version 29) provided statistical analysis of the exported survey data.
- The survey instrument assessed three key areas:
    - Participants' small-business cybersecurity experience (Table 7)
    - Perceived utility of the mindsets, in terms of enhancing respondents' understanding and improving their small-business cybersecurity engagement (Table 8)
    - Perceived validity of the mindsets (Table 9)

Tables 7, 8, and 9 follow. Each table includes the questions asked, their available response options, and each question's purpose.

Table 7: Questions Gathering Participants' Professional SME Experience

Question	Response Options	Inspiration Purpose
Which industry do you work in?	- Law enforcement - B2B consultancy - Cybersecurity consultancy - Other (please state)	Self-developed / Determine the participant's group affiliation (CRC or CSC)
In which SME category do you have the most experience working to improve cybersecurity?	- Micro (1–9 employees) - Small (10-49 employees) - Medium (49-249 employees) - I have equal experience across all SME categories	ONS and self-developed / To determine respondents' SME experience
Over your career, roughly how many of each SME category would you estimate you have engaged with regarding cybersecurity? (Select the most appropriate range for each category: micro, small, and medium.)	Micro / small / medium: - 50 or under - 51–100 - 101–150 - 151–200 - 201 or over	Self-developed / To determine respondents' SME experience

Table 8: Questions Gathering Data on Mindsets Utility

Question	Response Options	Inspiration / Purpose
To what extent do you think the mindsets are representative of micro, small, and medium businesses? (Select the most appropriate rating for each category.)	Micro / small / medium: - Not at all representative - Slightly representative - Moderately representative - Very representative - Extremely representative	Self-developed / Determine respondents' views on mindset validity
Were there any mindsets that stood out as being inaccurate?	- Yes: Which mindsets and why? (free text) - No	Self-developed / Determine respondents' views on mindset validity
Considering the recommendations for engaging each mindset, were there any that you think might be ineffective?	- Yes: Which mindsets and why? (free text) - No	Self-developed / Identify potential weaknesses in mindset-based engagement strategies
Do you think there are any engagement tactics missing from the recommendation section for a particular mindset that might help improve engagement?	- Yes: Which mindsets and why? (free text) - No	Self-developed / Identify potential weaknesses in mindset-based engagement strategies
As we conclude the survey, is there any additional feedback or clarifications you'd like to provide on topics that may not have been covered yet?	Free text (optional)	Self-developed / Capture any overlooked insights or unresolved questions

Table 9: Questions Gathering Data on Mindsets' Validity and Suitability of Recommendations

Question	**Response Options**	**Inspiration / Purpose**
To what extent do you think the mindsets are representative of micro, small, and medium businesses? (Select the most appropriate rating for each category.)	Micro / small / medium: - Not at all representative - Slightly representative - Moderately representative - Very representative - Extremely representative	Self-developed / Determine respondents' views on mindset validity
Were there any mindsets that stood out as being inaccurate?	- Yes: Which mindsets and why? (free text) - No	Self-developed / Determine respondents' views on mindset validity
Considering the recommendations for engaging each mindset, were there any that you think might be ineffective?	- Yes: Which mindsets and why? (free text) - No	Self-developed / Identify potential weaknesses in mindset-based engagement strategies
Do you think there are any engagement tactics missing from the recommendation section for a particular mindset that might help improve engagement?	- Yes: Which mindsets and why? (free text) - No	Self-developed / Identify potential weaknesses in mindset-based engagement strategies
As we conclude the survey, is there any additional feedback or clarifications you'd like to provide on topics that may not have been covered yet?	Free text (optional)	Self-developed / Capture any overlooked insights or unresolved questions

Survey Piloting and Administration Procedures

The survey was created using Qualtrics and underwent two iterative pilot rounds with 5 cybersecurity professionals in each round. Feedback focused on question clarity, logical flow, and minimizing cognitive load. Particular care was taken to avoid extended blocks of similar question types to reduce the risk of participant fatigue or response bias. The estimated completion time was 15 min, slightly longer than the often-cited optimal range of 8 min (Baxter et al., 2015). This trade-off was intentional, balancing data richness with response burden. Given the modest sample size (n = 20), it was considered an acceptable risk.

Prospective participants were emailed a combined participant information sheet and consent form that detailed the study's purpose, ethical safeguards, and voluntary participation. Upon providing consent, each participant received the following:

- a short explainer video (~5 min) introducing the concept of mindsets and the evaluation task
- a PDF pack containing the 8 prototype mindsets
- a personalized link to the anonymous Qualtrics survey

No incentives or compensation were provided for participation in this study.

Survey Data Analysis

We analyzed quantitative 5-point Likert scale data using descriptive statistics, presented as frequency counts and bar charts. Qualitative responses were synthesized using a structured framework that identified key patterns and organized insights into categories, including findings, impact, cause, and recommendation.

It is important to note that this paper's focus was on presenting our mindset creation method, which others can use to create their own mindsets; therefore, only the findings that present

insight into this objective are presented. Figure 18 summarizes participant recruitment, data collection, and analysis.

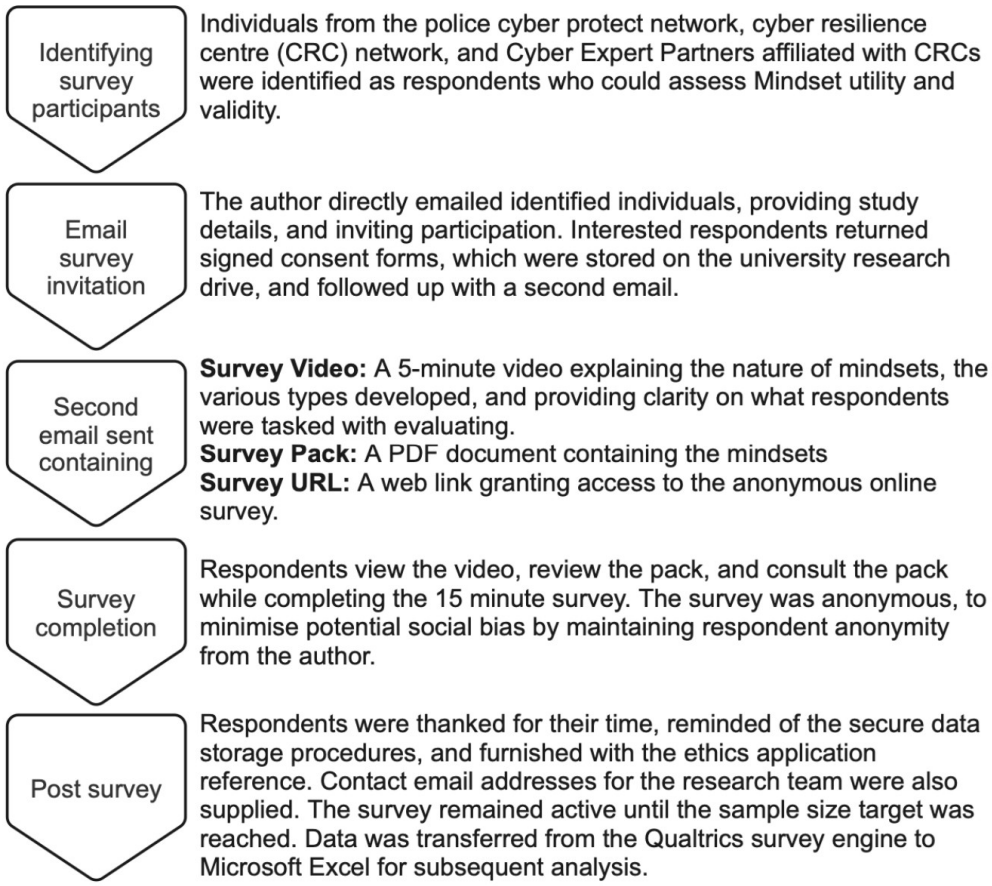

Figure 18: Participant recruitment, data collection, and analysis.

Results

Our results are presented in three parts. First, we provide a high-level summary of the Phase 1 thematic analysis, highlighting the top-level themes that informed mindset development. Second, we present the mindsets generated from this data using our six-step method. Third, we report findings from a survey with SME cybersecurity professionals who evaluated the perceived utility and validity of the resulting mindsets.

Phase 1 Thematic Analysis

Thematic analysis of interviews reveals eight major themes for DD (digitally dependent businesses that rely heavily on ICT), DB (digitally based businesses offering digital B2B services, excluding cybersecurity), and DE (digital enablers that are small-business cybersecurity consultants).

Risk perception factors: Participants' perceptions of their business's cyber risk (DD and DB) shaped these factors; for DEs, it was what they believed influenced small-business cyber risk judgments.

Engagement: The way that DD and DB participants sought cybersecurity guidance, and who assisted them, contributed to engagement. For DEs, engagement reflected how they approached small businesses, what prompted engagement, and their views on the guidance process.

Improvements: Participants made suggestions for how small-business cybersecurity engagement and adoption could be improved in the future.

Cues to action: Certain triggers prompted small businesses to adopt cybersecurity practices.

Engagement tactics: DEs used both effective and ineffective tactics to persuade small businesses to adopt cybersecurity (DE exclusively).

News: Participants formed certain views on how cybersecurity is portrayed in business media (DD and DB exclusively).

Return on investment (ROI): Participants assessed the value of cybersecurity and its potential return through ROI.

Cyber criminal perceptions: Participants' perceptions of hackers, in terms of characteristics or demographics (DD and DB exclusively), were a factor.

Figure 19 shows the interviewee count (IC) for each major theme, segmented by the DD, DB, and DE groups. Interviewee count (IC) refers to the number of individual interviewees who mentioned a particular theme at least once during their interview, which measured how widespread or commonly discussed a theme was across participants, regardless of how many times each person mentioned it. An asterisk shows a digital-enabler group-exclusive theme; two asterisks show digitally based and digitally-dependent group-exclusive themes.

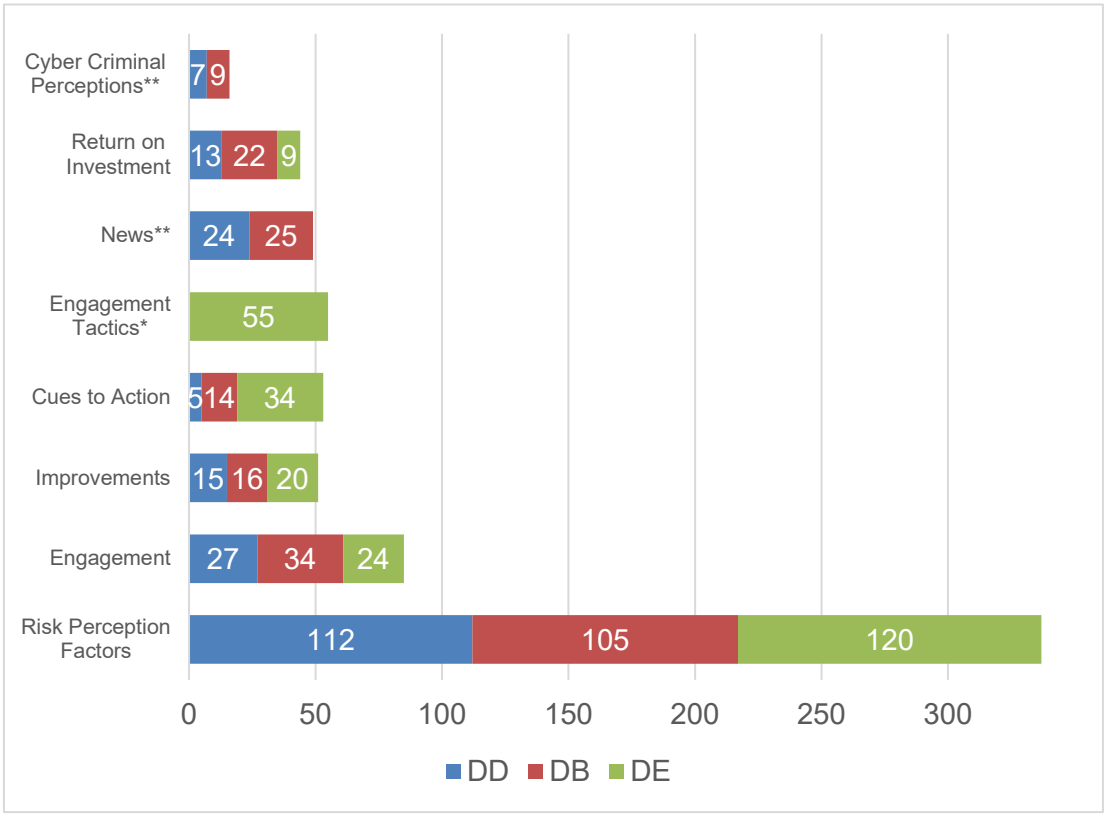

Figure 19: Grouped bar chart showing interviewee count (x-axis) against themes (y-axis), segmented by participant type.

Key Findings

Risk perception factors: The most dominant theme was risk perception, with 337 interviewees accounting for 49.1% of all theme-aligned quotations. Each group, DD (112), DB (105), and DE (120), contributed significantly, indicating that understanding and interpreting cyber risk was a consistent concern across all participant types. This aligns with broader findings in the field that small businesses often struggle to define or contextualize cyber risk in a business-relevant way (Osborn & Simpson, 2017).

Engagement and improvements: These themes followed distantly, with relatively balanced contributions from each group. However, DEs were more vocal in suggesting future improvements to cybersecurity engagement and adoption, which may reflect their role as external change agents with broader visibility across small businesses (Cartwright et al., 2023).

A notable imbalance appears in the cues to action theme: DEs contributed 34 ICs, whereas DDs contributed only 5. This aligns with existing literature suggesting that some small businesses, especially those with lower digital maturity, are less likely to recognize or act on cybersecurity triggers without external prompting (Tam et al., 2021).

Engagement tactics: This theme was exclusive to DEs, who contributed 55 ICs describing a range of tactics, both successful and unsuccessful, that they used to promote cybersecurity awareness and behavior change among small businesses.

News and cyber criminal perceptions: Exclusive to DD and DB groups, these themes received modest attention. The findings suggest that although participants did reference media coverage and stereotypical views of hackers, these were not primary influences shaping their actual cybersecurity behaviors (Bada et al., 2015).

Return on investment (ROI): All groups discussed ROI, but the theme was most prominent among DB participants (22 ICs). This may reflect DBs' reputational drivers, as for them, one of the key returns from investing in cybersecurity is protecting their business's public image and trustworthiness in the event of an attack (Kosutic, 2021).

Phase 2: Small-Business Cybersecurity Mindsets

Four mindsets were developed from the Phase 1 qualitative data using our six-step method.

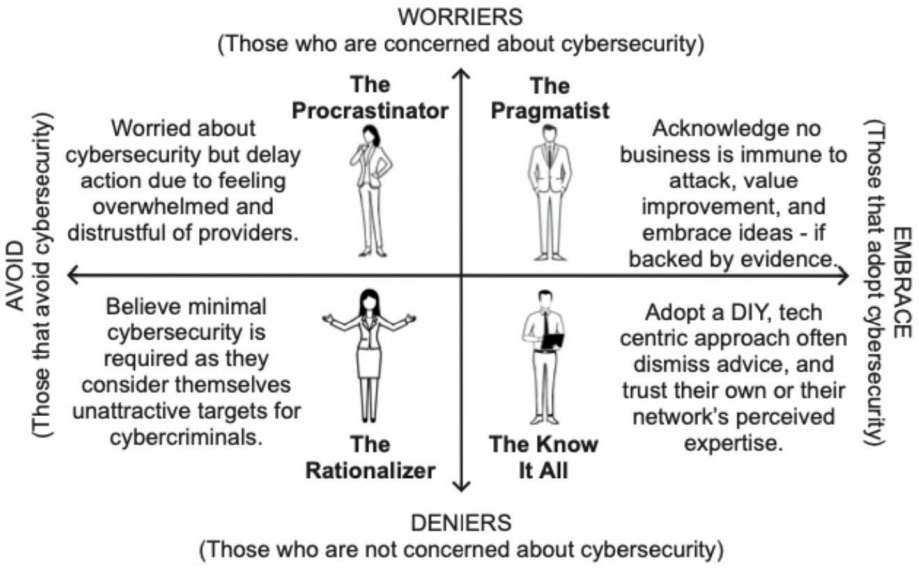

Figure 20: Mindsets produced from Phase 1 data.

The Procrastinator Mindset

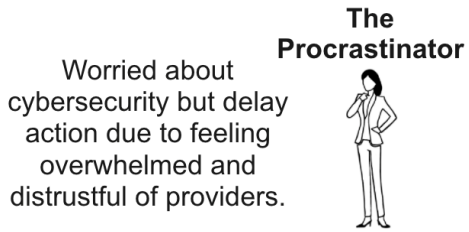

Figure 21: The Procrastinator.

Core beliefs:

- **Cyber risk is real but baffling.** They fear fraud (especially bank-data theft) yet admit, "I don't have a clue." They feel swamped by technical jargon and "information overload."
- **Providers look predatory.** Wary of being upsold, they think, "They'll just charge for extra support," and doubt they can "quantify a return" on any spend.

Typical behavior:

- **Delay and deflect.** Cyber jobs slide down the to-do list. It is "one of those things that gets left behind."
- **Tune-out.** Some avoid cyber news altogether.
- **Seek safe harbors.** When action is unavoidable, they favor smaller or mission-driven firms that they already trust.

Helping the procrastinator:

1. **Drop the scare tactics; speak plain English.** Replace fear appeals with simple, bite-sized guidance and deadlines.
2. **Nudge routinely and lock in commitments.** Regular emails and check-ins, plus pre-commitment tools (such as scheduled health checks and backup plans), keep momentum.
3. **Make it hands-on and fun.** Gamified tabletop drills—Cyber Lego®, Udder Disaster—turn boring tasks into engaged learning while exposing gaps.
4. **Point to neutral, low-cost help.** Refer them to government-backed CRCs or Police Protect Networks and offer limited free or discounted services; no hard sell.
5. **Show tangible ROI.** Track blocked attacks or customer-trust gains to prove security spend pays back.

The Rationalizer Mindset

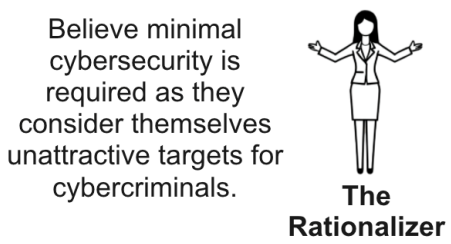

Figure 22: The Rationalizer.

Core beliefs:

- **"I'm not important:"** They think their data holds little value to attackers and attacks would be mere "headaches."
- **Habor stereotypical views of hackers:** It's just "a guy in a dark bedroom."
- **Security slows work:** Effort seems irrelevant unless proof of business impact is shown.
- **Hold myths:** "Apple can't be hacked," and they want evidence before acting.

Typical behavior:

- **Bare-minimum defenses:** They run the bare minimum, leaning on an IT supplier.
- **Ignore proactivity:** Unless they are forced by regulation, tenders, or a breach they will ignore problems.

Helping the procrastinator:

1. **Bust the myths:** Live demos or ICO incident stats show the prevalence of random, automated attacks.
2. **Walk in the hacker's shoes:** Exercises that reveal attacker motives make risks real.
3. **Provide reassurance:** Manage anxiety created from hack demos, give clear next steps (for example, cyber essentials), and frame action as progress, not failure.
4. **Anchor in trusted sources:** Point to NCSC, policing, or certified providers to build confidence.

The Pragmatist Mindset

Figure 23: The Pragmatist.

Core beliefs:

- **No business is 100 % safe:** Protection is considered a wise investment.
- **Lack cyber expertise and value certified partners:** They lack these resources.
- **Decisions should be data-driven:** They want to see ROI.

Typical behavior:

- **Proactive and open to advice:** They can continually fine-tune people, process, and tech approaches to cybersecurity.
- **Use trusted brands:** They like to use a brand like Crown Commercial Service or ISO-certified firms and ask for evidence of need.

Helping the pragmatist:

1. **Connect and share:** Point them to expos, webinars, and peer groups.
2. **Run a gap analysis:** Benchmark current supplier/support and highlight blind spots.
3. **Offer a roadmap:** Offer phased improvement plans and info on higher-level schemes (ISO 27001, IASME).
4. **Show the numbers:** Provide logs, phishing-click stats, or claim-reduction figures to prove impact.

The Know-It-All Mindset

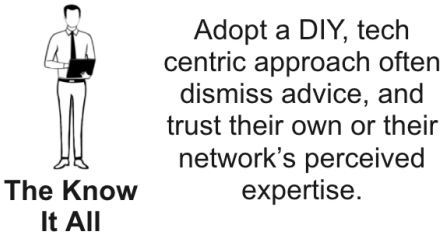

Figure 24: The Know-It-All.

Core beliefs:

- **Rate their cyber know-how above peers:** They trust an internal IT circle.
- **Overlook people/process gaps:** They equate "new tools" with full security.

Typical behavior:

- **Resist outside input:** They buy tech products and funnel advice back to in-house engineers.
- **Misaligned spend:** Their risk is in spending and stalled improvements.

Helping the know-it-all:

1. **Lead with authority, not argument:** Use NCSC or similar guidance that stresses policy, training, etc.
2. **Shift to risk language:** Frame gaps as business-risk controls, not tech specs.
3. **Trigger reputational stakes:** Case studies in which overconfident firms were breached hit home.
4. **Offer reality checks:** Objective assessments benchmarked against standards recalibrate self-view.
5. **Clarify skill boundaries:** Contrast IT support with certified cyber expertise (CE+, ISO 27001, or NCSC advisor).
6. **Table-top drills:** Hands-on incident simulations expose weaknesses without direct confrontation.

Mindset Evaluation Survey Results

We now present the findings of our mindset evaluation, beginning with the survey response rate, followed by participants' reported experiences with small-business cybersecurity. We then examine participant perceptions of the mindsets' utility and validity. Finally, we share insights from a synthesis of participants' free-text survey responses, organized by finding, impact, cause, and recommendation.

Survey Response Rate

Fifty-seven individuals belonging to the CRC and CSC groups were sent email invitations asking them to participate in the survey. Thirty-four responded by returning signed consent forms, totaling an initial 59.6% response rate. The 34 individuals were then sent a second email containing the prototype mindset artifacts, survey video, and an anonymous survey link. They completed the survey, which was closed after reaching the sample threshold of 20 (10 per CRC and CSC group), resulting in an overall response rate of 35.1%. As no statistically significant differences were found between the CRC and CSC groups' survey responses, results are reported at the global level. Where free-text comments are included, the verbatim quote is accompanied by an anonymous identifier (such as CRC1 or CSC2).

Respondent Professional Experience

Respondent experience is categorized by small business type (micro: 0-9 employees, small: 10-49 employees, medium: 50-249 employees, and equal: participants with comparable experience across all three categories). This includes both the category with which participants reported the most experience and an estimate of the number of businesses they had interacted with in each category. Figure 25 shows that 60% of participants indicated having equal experience across all business categories (micro, small, and medium). Meanwhile, 20% reported having the most experience working with small, 15% with medium, and 5% with micro.

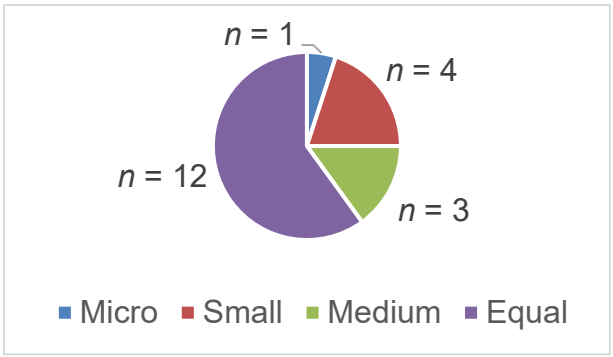

Figure 25: Pie chart illustrating the business categories most frequently engaged.

Figure 26 presents the reported number of business participants estimated to be engaging in cybersecurity.

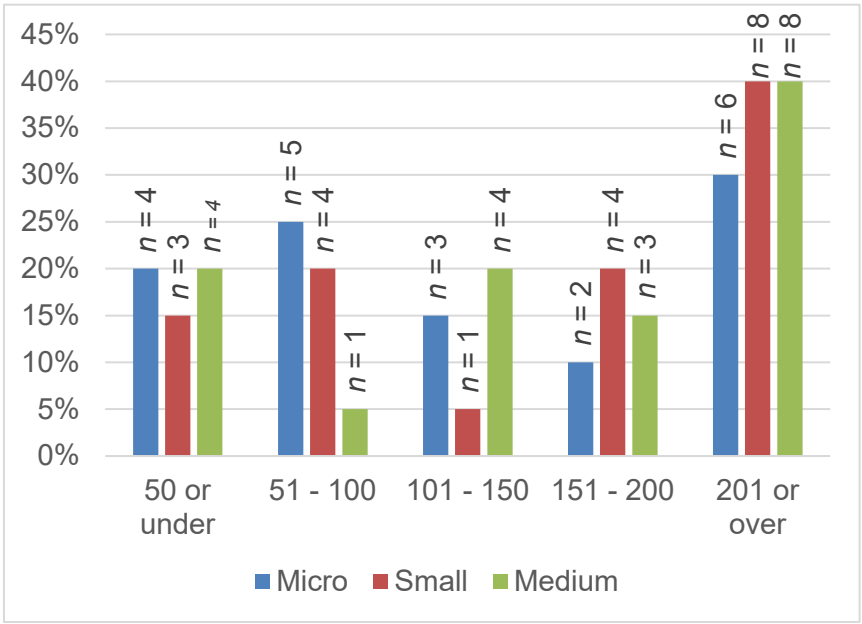

Figure 26: Total SMEs engaged with business size.

The data reveals that most participants reported significant experience with each small business size.

Perceived Representativeness of Mindsets

This section examines participants' perspectives on the validity (representativeness) of the mindsets, specifically, whether they accurately reflect the cybersecurity behaviors observed by consultants in the small businesses they had previously engaged. Understanding validity is important as it serves as a benchmark for determining whether the mindset accurately reflects real-world cybersecurity behaviors. Strong validity ratings increase confidence in the qualitative data collection methods and the process of converting that data into mindsets. Results are presented both visually and descriptively, incorporating free-text illustrative comments from participants as appropriate to provide deeper insights. Figure 27 shows participants' mindset validity ratings for micro, small, and medium-sized businesses.

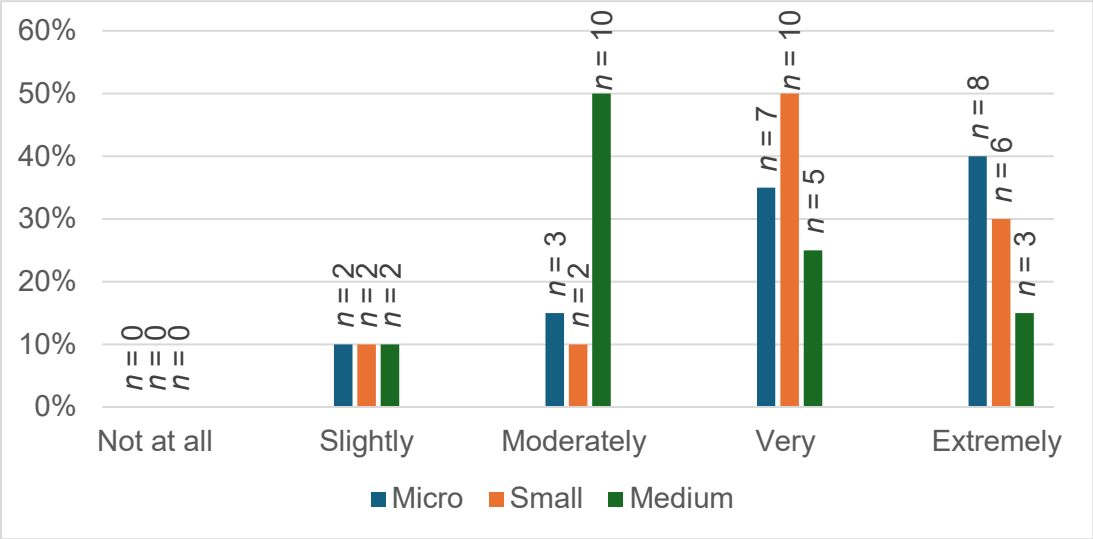

Figure 27: Participant mindset validity ratings (5-point Likert scale).

The results indicate strong perceived validity for micro and small businesses. Specifically, 80% (*n* = 16) of participants found the mindsets to be very or extremely representative of small businesses: "We have worked on the procrastinators as an organization in the past" (CSC6). Similarly, 75% (*n* = 15) reported the same for micro businesses. In contrast, only 40% (*n* = 8) rated the mindsets as highly representative of medium-sized businesses, with 50% (*n* = 10) indicating moderate alignment.

Usability and Applicability of Mindsets

This section presents participants' perceptions of the practical value of the mindsets in supporting cybersecurity engagement. The primary focus is on usability, that is, how easily participants were able to understand and apply the mindsets in practice. It also explores insights into whether participants felt the mindsets accurately reflected the behaviors and characteristics in the small business population.

Improving Participant Understanding and Potential for Enhancing Engagement

Figure 28 illustrates participants' perceptions of the mindset prototypes' potential to improve both their understanding of small-business cybersecurity attitudes and their ability to engage more effectively with small businesses in the future. The data shown here provides insight into how well the mindsets performed as practical tools, in terms of conceptual clarity, and also in their applicability for tailoring engagement strategies.

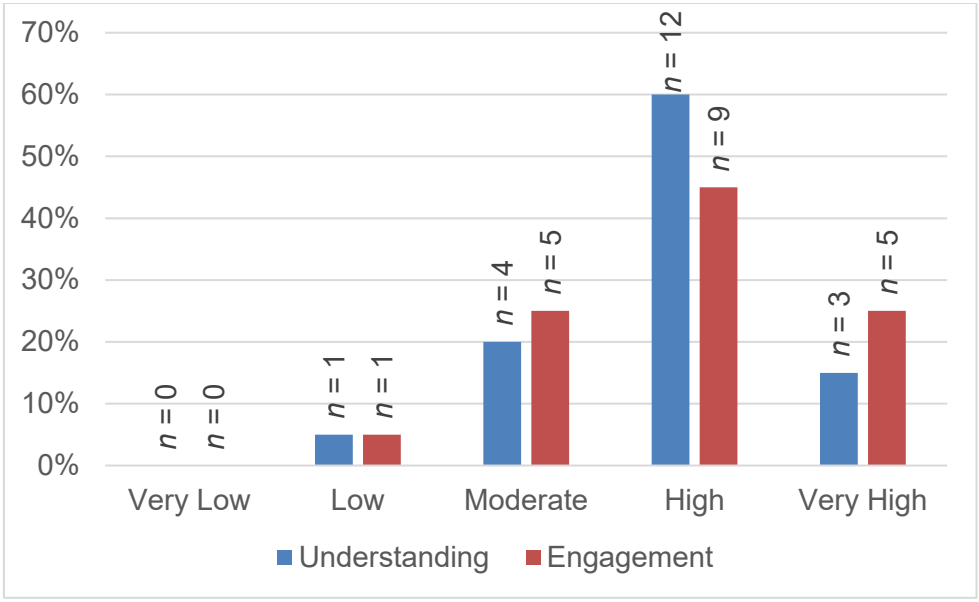

Figure 28: Survey responses on mindsets' potential to improve cybersecurity understanding and engagement.

The majority of participants, 75% (n = 15), felt the mindsets had high or very high potential to improve their understanding of small business cybersecurity. Similarly, 70% (n = 14) believed the mindsets could improve their ability to engage small businesses. As one participant noted, "If we understand what makes people engage, then we are more likely to encourage business change than other factors like business characteristics as a whole" (CRC2).

Some participants valued the psychological insights mindsets provided, which helped them understand small businesses better than comparing demographic-based segmentation: "People are individuals, not demographics" (CRC7).

Conversely, 5% (n = 1) of participants rated the mindsets as having low or very low potential to improve either understanding or engagement. This participant preferred more personalized methods, stating: "I still prefer to use a qualitative and individual engagement method" (CSC3).

Mindset Engagement Tactic Feedback

Figure 29 visualizes participant responses to three key questions evaluating the mindsets and their associated recommendations:

- Were any mindsets perceived as inaccurate?
- Were any of the recommended engagement tactics seen as potentially ineffective?
- Were any important engagement tactics missing from the recommendations?

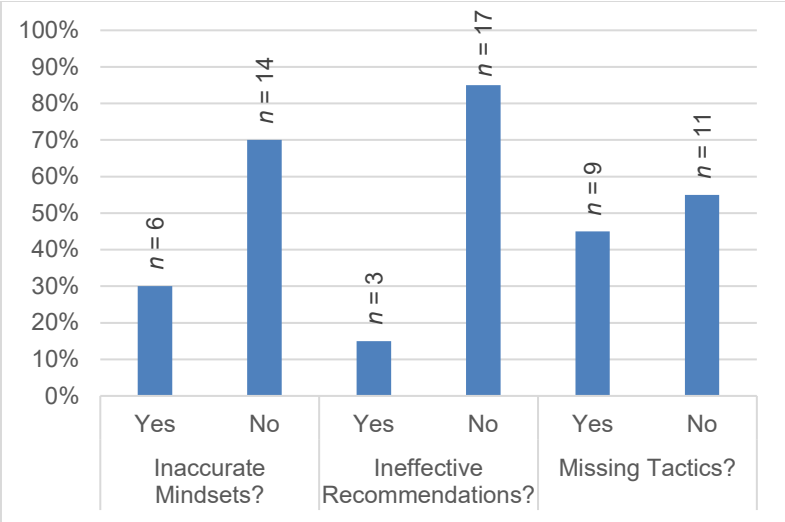

Figure 29: Survey responses regarding mindset accuracy, recommendation effectiveness, and missing engagement tactics.

Inaccurate Mindsets

Of the participants, 30% (*n* = 6) noted perceived issues with specific mindsets. However, comments primarily pointed to contextual limitations rather than inaccuracies in the mindsets themselves. For example, CRC7 commented that "larger businesses treat cybersecurity as someone else's problem," indicating that the concern was more about organizational dynamics than flaws in the mindsets. Notably, none of these comments raised issues relating to the validity of the mindsets.

Ineffective Recommendations

Of the participants, 15% (*n* = 3) raised concerns about the clarity and actionability of certain recommendations, particularly those related to emotional support. One respondent noted, "Emotional support suggested—probably need to unpack these recommendations more in terms of practical steps" (CSC1). These concerns were generally not about the validity of the recommendations themselves, but rather about their implementation. In the view of these participants, some recommendations needed to be made more explicitly actionable.

Missing Engagement Tactics

Of the participants, 45% (*n* = 9) suggested that certain engagement tactics were missing. Their feedback reflected practical application challenges, such as working with multiple mindsets (decision-makers) within the same organization, addressing passive or hard-to-reach SMEs, or tailoring approaches to larger businesses with different decision-making structures. For example, CRC9 asked: "How are these to be used with differing mindsets within the same organization?"

Although these comments offer valuable insights for mindset deployment within larger and more complex organizations, they do not critique the validity of mindsets. Rather, they highlight the need for additional guidance and flexibility in real-world implementation within the SME cybersecurity domain.

This concludes the analysis of quantitative survey data. The next section presents qualitative insights derived from participants' free-text comments.

Qualitative Insight Synthesis From Survey Free-Text Responses

Tables 10 (positive responses) and 11 (critical responses) present qualitative insights into mindset usability and validity using a structured format:

Finding: This column highlights what was noticed or reported during the evaluation, including key insights or observations drawn from participant free-text responses.

Impact: This column describes the potential consequence or effect of the finding, particularly in terms of how it influences the usability, effectiveness, or adoption of the mindsets.

Cause: This column identifies the underlying reason or contributing factor that explains why the finding occurred to provide context for the issue or success.

Recommendation: This column offers a practical, actionable suggestion for addressing the issue or building on the insight to improve future application or development of the mindsets.

Table 2: Summary of Positive Usability and Validity Insights From Survey Free-Text Responses

Finding	Impact	Cause	Recommendation
Five participants explicitly noted that the mindsets' evidence-based development increased their confidence in the tool's validity and credibility.	Practitioners are more likely to trust and adopt mindsets when they believe that they are grounded in data and are more science than art.	The survey participant pack included a brief explanation of the data sources and collection methods used to develop the mindsets.	Ensure users of mindsets understand how they were developed and the data behind them to build trust and support confident, consistent adoption.
Nine participants reported that the mindsets were easy to use.	Easy-to-use tools require minimal training, promote wider adoption, and reduce the risk of misapplication or misuse.	Snart and O'Connor's (2022) layouts ease cognitive load with simple formatting.	Consider using Snart and O'Connor's (2022) layout for a clearer, more usable mindset presentation.
Seven participants felt that the mindsets resonated with real-life SMEs they had previously encountered.	Valid mindsets lead to better decisions, stronger design impact, and deeper user alignment.	User needs, empathy mapping, and face validity questions adapted from Huynh et al. (2021) strengthened the overall validity of the mindsets.	Consider using these validation techniques during mindset creation.

Table 3: Summary of Critical Usability and Validity Insights From Survey Free-Text Responses

Finding	Impact	Cause	Recommendation
Six participants had difficulty determining which quadrant users should be placed into.	Misclassification could lead to ineffective engagement strategies.	Participants were not trained user researchers and had limited experience with user segmentation.	Provide a few targeted diagnostic questions* to guide practitioners toward the most appropriate mindset quadrant.
Five participants raised concerns that some mindset names might	Inappropriate mindsets may undermine stakeholder	The label know-it-all appeared to cause the most concern among participants.	Avoid controversial names if possible, but they may be justified if they clearly and

Finding	Impact	Cause	Recommendation
be inappropriate or potentially offensive.	engagement, especially in professional or diverse settings.		accurately reflect user behavior (for more detail, see our conclusion).
Five participants believed the mindsets might present a too simplistic view of human behavior.	If mindsets are seen as overly simplistic, users may question their credibility and hesitate to apply them in complex or nuanced situations.	Mindsets offer a high-level view of behaviors and actions, but participants may not have realized this and expected more granular detail.	Clarify that mindsets provide a high-level behavioral overview to help manage recipient expectations around detail and complexity.
Four participants raised concerns about applying the mindsets in contexts involving multiple decision-makers within the same organization.	Lack of confidence means the mindsets might be used in such circumstances or perhaps applied incorrectly.	Participants were unsure how to navigate situations in which influence is distributed across multiple stakeholders with potentially differing mindsets.	Identify the key decision-maker and apply their mindset, or tailor engagement to each stakeholder's mindset.
Two participants held concerns about the actionability of recommendations.	Inactionable recommendations may result in tactics not being used.	The concerns centered on one tactic in particular relating to emotional support.	Make sure recommendations are explicit and actionable.

* How concerned are you about cyber-attacks on your business, and can you explain why you're worried or not worried?
* Do you actively prioritize cybersecurity in your business, or do you tend to postpone or avoid it?

This concludes the quantitative and qualitative analysis of the evaluative survey. The conclusion now discusses these methodological findings in relation to existing literature.

Conclusion

We conclude by reflecting upon our mindset method findings in relation to existing literature and acknowledging key limitations, after which we outline directions for future research and present tips for user experience practitioners.

Reflections on the Six-Step Mindset Method

Step 1: Qualitative Data Reduction

The MECE process appears to be a highly suitable component within the overall mindset methodology. It proved invaluable for distilling dense qualitative data into clear, standalone components. By eliminating redundancy and preserving essential insights, MECE enhanced clarity and analytical focus. Its effectiveness in making data more digestible and understandable is well documented across domains such as finance (Henn et al., 2016) and sports (Ziye Wang et al., 2019), with comparative studies suggesting it outperforms other data reduction techniques (Lee & Chen, 2018). However, although such a reduction aids categorization, it might obscure the richness of lived experiences that qualitative research seeks to preserve.

Bowker and Star (1999) highlighted similar issues in the domain of thematic analysis, describing two coder types, lumpers who favor broader, more general themes, and splitters who favor more fine-grained categories. Lumpers risk losing nuance but offer clearer, more digestible insights, whereas splitters preserve detail but may fragment the data, making it less comprehensible. Bowker and Star suggested that the art lies in knowing when to lump and when to split, as each approach has merit depending on the research context and objectives.

This raises an important question: Which approach (lumping or splitting) is most suitable for mindset creation? A blog by System Concepts (2023) provides some insight, as it suggests that mindsets are ideal for capturing broad user attitudes and fostering high-level discussions, whereas personas are better suited to represent specific user needs and behaviors. From this perspective, a lumping approach, which is aligned with the MECE process, appears appropriate for mindsets, while a splitting approach may be better suited for persona development.

Step 2: Identifying Axes

A key limitation of this step is the inherent subjectivity involved in clustering or grouping data by similarity. Researchers may interpret and organize data differently depending on their perspectives or prior assumptions (Bowker & Star, 1999). In this study, such discrepancies were addressed through facilitating discussions between the authors to reach consensus. Although this approach helps mitigate bias, the subjective nature of clustering remains a recognized limitation of the method. Reflecting on this challenge, Lanning suggested that future iterations might benefit from facilitated workshops involving domain experts or stakeholders to collaboratively define the mindset axes, names, and overviews. Involving such expertise could strengthen the reliability of axis identification, arguably the most critical step in the process. Misidentifying these axes risks undermining the validity of the resulting mindsets.

Step 3: Placing Post-it Notes Into Mindset Quadrants

Lanning, as well as Clayton and O'Connor, recommended populating mindset quadrants with qualitative data, yet they offered limited guidance on how this should be carried out. Given ongoing criticism that design tools like personas and mindsets often rely too heavily on designer intuition (Cooper et al., 2014), we sought to address this limitation by developing a structured quadrant population method. This approach combines axis-based filtering, domain expertise, and reference to relevant literature to guide the placement of data within each quadrant. In doing so, it aligns with established best practices in design, which emphasize triangulating decisions against multiple sources of evidence (Cooper et al., 2014).

Step 4: Bringing Quadrants to Life

Once the qualitative data had been assigned to each quadrant, the focus shifted from classification to interpretation. This stage involved synthesizing beliefs and behaviors into coherent, relatable archetypes. We re-read the clustered Post-it notes aloud for each quadrant, asking two key questions:

- What motivates this group?
- What cybersecurity behaviors do they typically do, or avoid?

By exploring where motivation and action intersected, we surfaced a dominant character or mindset that captured the behavioral tendencies of that segment. This interpretive storytelling approach allows translating abstract tensions into intuitive, memorable archetypes, aligning with Clayton and O'Connor's recommendation that mindsets should be sticky and easy to recall. There was evidence that this goal was met. Nine participants praised the mindsets' usability, describing them as "easy to understand and relate to" (CSC1). One remarked, "It allows a deeper understanding into the mind of the buyer, enabling you to deal with each type in the correct manner" (CSC10). This feedback supports Lino and Bazoli's (2020) argument that effective design communication tools must engage both cognition and emotion to foster empathy and usability.

However, this step also introduces the following limitations.

RISK OF OVERSIMPLIFICATION

Five participants raised concerns that the mindsets may offer an overly simplistic view of small business cybersecurity: "The mindsets potentially provide an oversimplified view of the dilemmas faced by businesses" (CRC4). Such concerns are not unfounded. In translating rich qualitative data into concise archetypes, there is a risk of flattening complexity or ignoring edge cases. Yet, mindsets are deliberately designed to communicate broad, high-level behavioral tendencies, something System Concepts (2023) describes as a "helicopter view." This stands in contrast to personas, which are better suited for detailed representation of specific user types.

Although oversimplification is a valid concern, our intention was to prioritize accessibility and practical utility for non-researchers working with small businesses.

Concerns About Stereotyping

A related issue is the perceived bluntness of the mindset names. Five participants suggested that more neutral or politically correct labels might be preferable: the "know-it-all" or "procrastinator" could be interpreted as pejorative. This reflects a broader tension in persona design: the need for intuitive, impactful labels versus reinforcing negative stereotypes. Our choice of names was guided by the principle of memorability. Research shows that stereotypical naming, when grounded in data, can aid recall and communication (Nitafan, 2019). Turner and Turner (2011) argued that stereotypes in UCD are not inherently harmful if they are evidence-based and free from personal bias. Similarly, Conrad (1972) suggested that stereotypes offer cognitive efficiency, enabling faster categorization and decision-making. We acknowledge the risks, but we contend that, in our case, the names are empirically derived and function as mnemonic tools rather than prejudicial labels. Nonetheless, future applications of the method might explore offering both evocative and neutral names depending on the audience and use case.

Step 5: Engagement Tactics

A key challenge in mindset creation is not only in identifying relevant engagement tactics but also in ensuring they are accurately mapped to the most appropriate mindset quadrant. This two-part process requires both insight and rigor. To identify effective tactics, it is useful to draw on two main sources. First, as Lanning suggested, seek the expertise of those who deeply understand the target user group, such as domain experts or practitioners with lived experience. Second, consult the academic and gray literature to uncover evidence-based strategies that have been shown to work with similar user segments. This helps ensure that tactics are not invented in a vacuum but are grounded in existing knowledge.

Once tactics are identified, the next step is assigning them to the correct mindset. This must be done carefully to avoid arbitrary or overly subjective placement. We recommend that every assignment be justified through either domain insight or literature. For instance, Wilson et al. (2022) proposed tactics to counter the misconception held by many small businesses that "I'm too small to be attacked," a belief aligned with our rationalizer mindset. It is therefore logical to apply those tactics directly to that mindset, ensuring both conceptual alignment and practical relevance.

Despite our best efforts, some participants felt that the engagement guidance lacked actionable detail. For example, one participant (CSC1) commented: "Emotional support suggested for rationalizers: Probably need to unpack these recommendations more in terms of practical steps." This feedback reinforces a key insight: For mindset-based recommendations to be effective in real-world settings, they must be clear, specific, and implementable. This finding aligns with behavior-change literature. Albarracín et al. (2018), for example, showed that interventions are more successful when they include specific, action-oriented steps rather than vague or abstract suggestions. Thus, when crafting mindset engagement tactics, we recommend designers ensure they ground in evidence, map with intention, and present in ways that end users can immediately apply.

Step 6: Face Validity Checks

The importance of conducting robust validation is well-established. Chapman and Milham (2006), for example, cautioned that without empirical grounding and systematic evaluation, design tools like personas, and by extension, mindsets, could become stereotypical or superficial. To address this methodological gap, we incorporated two face validity questions inspired by Huynh et al. (2021). These questions aimed to quickly assess whether the mindsets not only reflected the underlying qualitative data but also resonated with the lived experiences of intended users.

The results are encouraging. Free-text survey comments indicated that participants found the mindsets intuitive and grounded in real-world business realities. One participant remarked, "We have worked on the procrastinators as an organization in the past" (CSC6), signaling strong recognition. Quantitatively, 80% of respondents (n = 16) said the mindsets were highly or

extremely representative of small businesses, and 75% (n = 15) said the same for micro-businesses. However, this pattern did not extend to medium-sized businesses. Only 50% (n = 10) found the mindsets moderately aligned with that group. This raises an important question: Why was perceived validity lower for medium-sized enterprises?

The most plausible explanation is in the study's sampling frame. The mindsets were developed using interview data from 18 micro-businesses and just 2 small businesses, with no direct input from medium-sized enterprises. Therefore, their limited applicability to this segment is both understandable and expected. Importantly, the original aim of this study was to develop mindsets specifically for micro and small businesses, not medium-sized ones. From this perspective, high alignment with medium-sized businesses might actually be a red flag. It could suggest participant bias (such as overly positive feedback) or raise concerns about methodological overreach and overgeneralization. This trend is echoed in the literature. Although micro and small businesses often share similar characteristics, medium-sized businesses are typically quite different, particularly in their cybersecurity infrastructure, practices, and resources (Sytnik & Kravchenko, 2021). As such, strong alignment with medium-sized businesses would have been unexpected and potentially confounding.

This concludes this discussion of our findings. We now turn to future research opportunities that could strengthen the method presented in this paper, after which we present tips for user experience practitioners who may wish to apply our method to create their own mindsets.

Future Research

Future research should address the limitation of this study's small evaluation sample (n = 20); a natural next step is to deploy the mindsets developed in this study in real-world settings, for example, by sharing them with cybersecurity professionals and conducting longitudinal studies with small businesses. Such research could provide deeper insight into how the mindsets support cybersecurity engagement, reveal opportunities for refinement, and offer a more robust evaluation of their validity and effectiveness in influencing behavior and decision-making in everyday practice.

Tips for User Experience Practitioners

- When analyzing qualitative data to develop mindsets, begin by sorting insights into two broad categories: beliefs and actions. This early separation helps surface the kinds of opposing patterns needed to define meaningful axes, because each axis typically contrasts belief types or behavioral tendencies.
- Consult domain experts to identify practical engagement tactics and ensure these are accurately aligned with the appropriate mindset quadrant. Their contextual knowledge can help avoid mismatches and enhance the relevance and effectiveness of your recommendations.
- Because mindsets are a relatively new communication tool in UCD, they may be unfamiliar to some design teams. To build trust and credibility, consider sharing a concise explanation of how your mindsets were developed, including the data sources and methodology behind them.

Acknowledgements

We extend our sincere thanks to the UK CRC Network, all study participants, and the faculty and researchers at Abertay University, Dundee, for their valuable feedback and contributions to this work. We also gratefully acknowledge Christina Lanning and Code for Canada for permission to reuse and adapt their figures, as well as Jo Clayton and Marc O'Connor for permission to reuse and adapt HMRC figures in this publication.

References

Accenture. (2019). *Designing the financial services of the future: Mindset segmentation*. https://web.archive.org/web/20220117212653/https://mindsets.fjordnet.com/reaching-the-mindsets

Albarracín, D., Wilson, K., Chan, M.-S., Durantini, M., & Sanchez, F. (2018). Action and inaction in multi-behaviour recommendations: A meta-analysis of lifestyle interventions. *Health Psychology Review*, *12*(1), 1–24. https://doi.org/10.1080/17437199.2017.1369140

Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society*, *73*, 102258. https://doi.org/10.1016/j.techsoc.2023.102258

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv*, 118–131. https://doi.org/10.48550/arXiv.1901.02672

Baum, N. (2020). Patient profiling using psychographics: Demographics vs. psychographics and why culture matters most. *The Journal of Medical Practice Management*, *35*(4), 234–236.

Baxter, K., Courage, C., & Caine, K. (2015). *Understanding your users: A practical guide to user research methods*. Morgan Kaufmann.

Bernard, H. R. (2017). *Research methods in anthropology: Qualitative and quantitative approaches*. Rowman & Littlefield.

Bowker, G. C., & Star, S. L. (1999). *Sorting things out: Classification and its consequences*. The MIT Press. https://doi.org/10.7551/mitpress/6352.001.0001

Bowling, A., & Ebrahim, S. (2005). *Handbook of health research methods: Investigation, measurement and analysis*. McGraw-Hill Education. https://books.google.co.uk/books?id=_HznvwUxkZsC

Carter, S., & Henderson, L. (2005). Approaches to qualitative data collection in social science. In A. Bowling & S. Ebrahim (Eds.), *Handbook of health research methods: Investigation, measurement and analysis* (pp. 215–230). McGraw-Hill Education.

Cartwright, A., Cartwright, E., & Edun, E. (2023). Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies. *Computers & Security*, 103288. https://doi.org/10.1016/j.cose.2023.103288

Chapman, C. N., & Milham, R. P. (2006). The personas' new clothes: Methodological and practical arguments against a popular method. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *50*(5), 634–636. https://doi.org/10.1177/154193120605000503

Claar, C. L. (2011). *The adoption of computer security: An analysis of home personal computer user behavior using the health belief model* [Master's thesis]. Utah State University. https://digitalcommons.usu.edu/etd/878

Conrad, C. (1972). Cognitive economy in semantic memory. *Journal of Experimental Psychology*, *92*, 149–154. https://doi.org/10.1037/h0032072

Cooper, A. (1999). The inmates are running the asylum. In U. Arend, E. Eberleh, & K. Pitschke (Eds.), *Software-Ergonomie '99: Design von Informationswelten* (p. 17). Vieweg+Teubner Verlag. https://doi.org/10.1007/978-3-322-99786-9_1

Cooper, A., Reimann, R., Cronin, D., & Noessel, C. (2014). *About face: The essentials of interaction design*. John Wiley & Sons.

Frost, J., & Hendrick, B. (2020, December 2). *Understanding and designing for changing mindsets during a global pandemic*. https://digital.canada.ca/2020/12/02/understanding-and-designing-for-changing-mindsets-during-a-global-pandemic/

Henn, L., Sloan, K., Charles, M. B., & Douglas, N. (2016). An appraisal framework for evaluating financing approaches for public infrastructure. *Public Money & Management*, *36*(4), 273–280. https://doi.org/10.1080/09540962.2016.1162595

Howard, T. W. (2015). Are personas really usable? *Communication Design Quarterly*, *3*(2), 20–26. https://doi.org/10.1145/2752853.2752856

Huynh, T., Madsen, A., McKagan, S., & Sayre, E. (2021). Building personas from phenomenography: A method for user-centered design in education. *Information and Learning Sciences*, *122*(11/12), 689–708.

Khan, N., Furnell, S., Bada, M., Rand, M., & Nurse, J. R. C. (2025). Investigating the experiences of providing cyber security support to small- and medium-sized enterprises. *Computers & Security*, *154*, 104448. https://doi.org/10.1016/j.cose.2025.104448

Kosutic, D. (2021). *The impact of cybersecurity on competitive advantage* [Student thesis, Grenoble Ecole de Management]. https://www.researchgate.net/profile/Dejan-Kosutic-2/publication/357826918_The_Impact_of_Cybersecurity_on_Competitive_Advantage/links/61e143d270db8b034c92052e/The-Impact-of-Cybersecurity-on-Competitive-Advantage.pdf

Kotler, P., & Armstrong, G. (1999). *Principles of marketing* (8th ed.). Prentice Hall. https://books.google.co.uk/books?id=AxKVQgAACAAJ

Landis, J. R., & Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics*, *33*(1), 159–174. JSTOR. https://doi.org/10.2307/2529310

Lanning, C. (2021). *Hello mindsets! A new way to understand users*. https://codefor.ca/blog/hello-mindsets-a-new-way-to-understand-your-users/

Larson, R. B. (2019). Controlling social desirability bias. *International Journal of Market Research*, *61*(5), 534–547. https://doi.org/10.1177/1470785318805305

Lee, C.-Y., & Chen, B.-S. (2018). Mutually-exclusive-and-collectively-exhaustive feature selection scheme. *Applied Soft Computing*, *68*, 961–971. https://doi.org/10.1016/j.asoc.2017.04.055

Lino, C., & Bazoli, G. (2020, February 6). *Mindset over matter: A new design trick for your toolbox*. https://www.designit.com/stories/point-of-view/mindset-over-matter-part-three

Marsh, S. (2022). *User research: Improve product and service design and enhance your UX research* (2nd ed.). Kogan Page.

Minto, B. (2021). *The pyramid principle: Logic in writing and thinking* (3rd ed.). FT Publishing International.

Morgan, D. L. (1997). *Focus groups as qualitative research* (2nd ed.). Sage Publications.

Mulder, S., & Yaar, Z. (2007). Approaches to creating personas. *The user is always right: A practical guide to creating and using personas for the web* (pp. 33–54). New Riders.

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (Calvin). (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815–825. https://doi.org/10.1016/j.dss.2008.11.010

Nielsen, T. (2021, May 5). *Personas versus mindsets*. LinkedIn. https://www.linkedin.com/pulse/personas-versus-mindsets-tina-m%C3%B8rch-nielsen/

Nielson, J. (2012, June 3). *How many test users in a usability study?* Nielson Norman Group. https://www.nngroup.com/articles/how-many-test-users/

Nitafan, E. (2019, December 10). *Design your products around mindsets, not just user personas*. Medium. https://medium.com/swlh/design-your-products-around-mindsets-not-just-user-personas-68b1b6f35f85

Osborn, D., & Simpson, A. (2017). Risk and the small-scale cyber security decision making dialogue—A UK case study. *The Computer Journal*, *61*(4), 472–495. https://doi.org/10.1093/comjnl/bxx093

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research*, *42*(5), 533–544. https://doi.org/10.1007/s10488-013-0528-y

Patton, M. Q. (2002). *Qualitative research and evaluation methods* (3rd ed.). Sage Publications.

Rosenstock, I. M., Strecher, V. J., & Becker, M. H. (1988). Social learning theory and the health belief model. *Health Education Quarterly*, *15*(2), 175–183. https://doi.org/10.1177/109019818801500203

Salminen, J., Jansen, B. J., An, J., Kwak, H., & Jung, S.-G. (2018). Are personas done? Evaluating the usefulness of personas in the age of online analytics. *Persona Studies*, *4*(2).

Salminen, J., Jung, S., Nielsen, L., Şengün, S., & Jansen, B. J. (2022). How does varying the number of personas affect user perceptions and behavior? Challenging the "small personas" hypothesis! *International Journal of Human-Computer Studies*, *168*, 102915. https://doi.org/10.1016/j.ijhcs.2022.102915

Salminen, J., Jung, S.-G., Chowdhury, S., Robillos, D. R., & Jansen, B. (2021). The ability of personas: An empirical evaluation of altering incorrect preconceptions about users. *International Journal of Human-Computer Studies*, *153*, 102645. https://doi.org/10.1016/j.ijhcs.2021.102645

SBS. (2020). *The EU Cybersecurity Act and the role of standards for SMEs: Position paper*. European DIGITAL SME Alliance. https://www.sbs-sme.eu/sites/default/files/publications/23032020%20SBS%20Position%20Paper_EU%20Cybersecurity%20Act%20and%20the%20role%20of%20standards%20for%20SMEs.pdf

Snart, J., & O'Connor. (2022). *Mindsets vs personas* [Conference presentation]. Service Design in Government (SDinGov) [on behalf of HMRC]. https://govservicedesign.net/programme/mindsets-vs-personas

Steel, P. (2010). Arousal, avoidant and decisional procrastinators: Do they exist? *Personality and Individual Differences*, *48*(8), 926–934. https://doi.org/10.1016/j.paid.2010.02.025

System Concepts. (2023). *Are mindsets the new personas*? https://www.system-concepts.com/insights/are-mindsets-the-new-personas/

Sytnik, N., & Kravchenko, M. (2021). Application of knowledge management tools: Comparative analysis of small, medium, and large enterprises. *Journal of Entrepreneurship, Management and Innovation*, *17*(4), 121–156. https://doi.org/10.7341/20211745

Tam, T., Rao, A., & Hall, J. (2021). The good, the bad and the missing: A narrative review of cyber-security implications for Australian small businesses. *Computers & Security*, *109*, 102385. https://doi.org/10.1016/j.cose.2021.102385

Tebb, K. P., Erenrich, R. K., Jasik, C. B., Berna, M. S., Lester, J. C., & Ozer, E. M. (2016). Use of theory in computer-based interventions to reduce alcohol use among adolescents and young adults: A systematic review. *BMC Public Health*, *16*(1), 1–33. https://doi.org/10.1186/s12889-016-3183-x

Turner, P., & Turner, S. (2011). Is stereotyping inevitable when designing with personas? *Design Studies*, *32*(1), 30–44. https://doi.org/10.1016/j.destud.2010.06.002

Wilson, M., & McDonald, S. (2024). One size does not fit all: Exploring the cybersecurity perspectives and engagement preferences of UK-based small businesses. *Information Security Journal: A Global Perspective*, *34*(1), 15–49. https://doi.org/10.1080/19393555.2024.2357310

Wilson, M., McDonald, S., Button, D., & McGarry, K. (2022). It won't happen to me: Surveying SME attitudes to cyber-security. *Journal of Computer Information Systems*, 1–13. https://doi.org/10.1080/08874417.2022.2067791

Wang, Z., Feng, S., & Zhao, X. (2019). MECE method and its application in sports event interpretation. *Proceedings of the First International Symposium on Management and Social Sciences (ISMSS 2019)* (pp. 340–343). https://doi.org/10.2991/ismss-19.2019.73

About the Authors

Dr. Martin Wilson
Dr. Martin Wilson is a serving UK police officer and Deputy Director of the North East Cyber Resilience Centre. He is a cybersecurity leader with over 20 years of experience and a published PhD researcher specializing in user-centered design and cybersecurity. He advises senior stakeholders across government and industry, supporting the delivery of inclusive, human-centered solutions.

Professor Alastair Irons
Professor Alastair Irons is an Emeritus Professor of Computer Science and Vice President of BCS. A National Teaching Fellow, he has held senior roles at Abertay and Sunderland and is a visiting professor in Egypt and South Africa. He also serves on several national and international digital and education boards.

Sharon McDonald
Sharon McDonald is a Lead User Researcher in the Government Digital Service, where she has led user research on a number of high-profile teams and products. She has a PhD in Cognitive Psychology from the University of Durham and is a Chartered Psychologist.