

Behaviour & Information Technology

ISSN: 0144-929X (Print) 1362-3001 (Online) Journal homepage: www.tandfonline.com/journals/tbit20

What micro-businesses need: a user-centered approach to cybersecurity support

Martin Wilson, Sharon Mcdonald, Alastair Irons & Joe Cockcroft

To cite this article: Martin Wilson, Sharon Mcdonald, Alastair Irons & Joe Cockcroft (21 Jun 2026): What micro-businesses need: a user-centered approach to cybersecurity support, Behaviour & Information Technology, DOI: 10.1080/0144929X.2026.2686166

To link to this article: https://doi.org/10.1080/0144929X.2026.2686166

© 2026 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group

Published online: 21 Jun 2026.

Submit your article to this journal

Article views: 11

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=tbit20

BEHAVIOUR & INFORMATION TECHNOLOGY
https://doi.org/10.1080/0144929X.2026.2686166

Taylor & Francis
by informa

OPEN ACCESS Check for updates

What micro-businesses need: a user-centered approach to cybersecurity support

Martin Wilson [a], Sharon Mcdonald [b], Alastair Irons [a] and Joe Cockcroft [c]

[a]School of Design and Informatics, Division of Cybersecurity, Abertay University, Dundee, UK; [b]Government Digital Service, London, UK; [c]Layer 7 Limited, Ashington, UK

ABSTRACT

Micro-businesses are disproportionately exposed to cyber threats yet remain underserved by generic 'one size fits all' cybersecurity guidance that often fails to reflect their resource constraints and operational realities. To address this research-practice gap, this study adopts a user-centered design (UCD) approach to synthesise and articulate the cybersecurity needs of UK micro-businesses. Thirty semi-structured interviews were conducted across three subgroups: Digitally Dependent, Digitally Based, and Digital Enablers. Thematic analysis generated 36 user needs, expressed using the UK Government Digital Service (GDS) format and organised into four categories: Guidance, Posture, Resources, and Return on Investment (ROI). Guidance needs were most prominent, highlighting demand for actionable, simple, tailored, and trustworthy support that reaches businesses proactively, avoiding fear appeals. While resource constraints were universal, subgroup differences emerged particularly in ROI and regulatory awareness, underscoring the limitations of homogeneous SME engagement strategies. Rather than offering new findings on barriers to adoption or proposing empirically validated interventions, the study contributes a structured, user-needs-led benchmark and a literature-informed 'opportunity space' for designing more contextually aligned cybersecurity support. Overall, the findings suggest that improving SME cybersecurity engagement may depend less on generating new knowledge and more on translating existing insights into accessible, actionable, and user-aligned forms of support.

ARTICLE HISTORY
Received 10 October 2025
Accepted 2 June 2026

KEYWORDS
Cybersecurity; micro-businesses; small and medium enterprises (SMEs); user-centered design; user needs; cybersecurity adoption

1. Introduction

This study aims to identify and articulate the cybersecurity needs of UK micro-businesses by: (1) eliciting user needs through interviews and translating these insights into an actionable, accessible benchmark expressed in the voice of micro-business owners; (2) examining how these needs differ across micro-business subgroups (Digitally Dependent and Digitally Based), while drawing on insights from Digital Enablers (e.g. SME cybersecurity consultants to provide provider perspectives to contextualise) and triangulate the findings, rather than treating them as direct representations of micro-business user needs; and (3) reviewing literature-informed approaches that may address the identified needs. In doing so, the study contributes a design-oriented benchmark of micro-business user needs to support policymakers, practitioners, and researchers in tailoring interventions beyond 'one size fits all' guidance.

This focus is important because SMEs, particularly micro-businesses, are economically important yet increasingly digitally exposed. SMEs account for 99% of UK private businesses, 60% of employment, and 50% of turnover (Federation of Small Businesses 2023). According to the Companies Act (2006), micro-enterprises employ fewer than 10 staff, small enterprises 11–50, and medium enterprises 51–250 (UK Government 2006). As most UK SMEs fall within the micro-business category, and most start-ups begin as micro-enterprises, the resilience of this subgroup is strategically significant (DBT 2024). This centrality is mirrored globally, with SMEs forming the backbone of most economies and driving employment, innovation, and growth (Aranitou and Arachovas 2024).

At the same time, SMEs' reliance on digital technologies has intensified due to post-COVID shifts to online working and accelerated digitalisation (Klein and Todesco 2020). The UK Cyber Security Breaches Survey (2024) highlights the extent of this trend, reporting that 91% of SMEs are digitally exposed through activities such as online banking, customer data storage, smart devices, and e-commerce (DSIT 2024). While increased

CONTACT Martin Wilson martin.wilson@nebrcentre.co.uk School of Design and Informatics, Division of Cybersecurity, Abertay University, Kydd Building, 40 Bell Street, Dundee, UK

© 2026 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group
This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (http://creativecommons.org/licenses/by-nc-nd/4.0/), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

digitisation offers operational benefits, it also expands SMEs' digital footprint and associated attack surface, heightening vulnerability to cyber-attacks (Alahmari and Duncan 2020). Accordingly, this study begins by examining the prevalence of cyber-attacks affecting small and micro-businesses alongside their appraisals of cyber risk.

1.1. Cyber attacks and risk appraisal in SMEs

Small businesses remain frequent targets of cyber-attacks, with 43% reporting incidents in the 2025 UK Cyber Security Breaches Survey (DSIT 2025b). Since the survey's inception in 2016, this proportion has remained relatively stable, fluctuating between 32% and 50% annually. Extant research highlights a persistent juxtaposition between SMEs' sustained exposure to cyber threats and their comparatively low perceived personal risk (e.g. Button et al. 2026; Rawindaran et al. 2023; Saban, Rau, and Wood 2021). Osborn and Simpson (2018) characterise this mindset as a form of 'security in obscurity', whereby SMEs perceive themselves as unlikely targets, assume they possess little of value, and therefore deprioritize protective action. This suggests a largely superficial understanding of attacker motives and methods (Bitzer, Stahl, and Strobel 2021).

This limited risk appraisal may help explain why, despite continued victimisation rates, SMEs frequently deprioritize cybersecurity investment and preparedness (Hoppe, Gatzert, and Gruner 2021). Regardless of perceived risk, however, the consequences of cyber incidents for SMEs can be substantial (Saha and Anwar 2024). Attacks may disrupt operations, compromise financial stability, damage organisational reputation, generate legal and regulatory liabilities, and weaken supply chain relationships; in severe cases, they may even threaten organisational survival (Haney and Lutters 2018; Wolf, Aviv, and Kuber 2021). These potential impacts underscore the importance of proactive cybersecurity practices, which we now explore further.

1.2. Implementation of protective controls

Existing literature indicates that SMEs demonstrate limited and uneven implementation of protective cybersecurity controls, resulting in suboptimal security postures (Chidukwani, Zander, and Koutsakis 2026). Many firms rely on basic safeguards, such as passwords, while underutilising more robust controls including multi-factor authentication, regular patching, and structured backup processes (Ncubukezi, Mwansa, and Rocaries 2020). Osborn and Simpson (2018) interpret this pattern as symptomatic of a predominantly technology-centric approach, whereby SMEs adopt isolated technical tools rather than implementing a holistic cybersecurity strategy.

Such approaches are often linked to limited cybersecurity knowledge, constrained in-house expertise, resource pressures, and low awareness of best practice (Cartwright and Cartwright 2025). Consequently, the broader principles of best-practice cybersecurity, particularly the integrated focus on people, processes, and technology, are frequently overlooked, resulting in uneven organisational resilience. The literature also reflects ongoing debate regarding the suitability of established cybersecurity frameworks for SMEs. Tam, Rao, and Hall (2021) argue that many frameworks are designed for larger organisations and are therefore overly complex and resource-intensive for SME contexts. Some researchers advocate the development of lightweight, SME-specific frameworks tailored to organisational constraints (Rae and Patel 2019), while others recommend adapting existing standards to improve contextual fit (Van Haastrecht et al. 2021). However, empirical evidence evaluating the effectiveness of either approach remains limited.

In the UK, government-backed initiatives such as the Cyber Essentials scheme promote the adoption of baseline protective controls capable of mitigating common automated cyber-attacks (Such et al. 2019). Nevertheless, uptake has remained comparatively low, as evidenced by successive UK Cyber Security Breaches Surveys showing that SME awareness of Cyber Essentials has remained modest and, in some years, declined, particularly among micro-businesses. This indicates a persistent gap between the availability of best-practice guidance and meaningful organisational engagement with, and implementation of, recommended security measures. The following section examines the antecedents of this limited uptake.

1.3. Barriers to cybersecurity guidance uptake

The literature identifies multiple factors contributing to the limited uptake of cybersecurity measures among SMEs. A lack of awareness remains a significant barrier, with many firms simply unaware of available guidance and support (Khan et al. 2025a; Khan et al. 2026). Resource constraints further compound this challenge, as limited time, finances, and in-house expertise make it difficult to prioritise cybersecurity (Alahmari and Duncan 2021; Wilson et al. 2023). These pressures are exacerbated by business leaders' difficulties in articulating, or even recognising, the return on investment (ROI) associated with cybersecurity (Kosutic and Pigni 2022), despite evidence that it can function as a strategic enabler and source of competitive advantage (Barlette, Gundolf, and Jaouen 2017). Under such conditions, cybersecurity is

frequently deprioritized when its value is perceived as indirect or uncertain (Hoppe, Gatzert, and Gruner 2021).

SMEs also tend to rely on informal networks and word-of-mouth for cybersecurity guidance (Renaud and Ophoff 2021), which can be problematic when advice originates from individuals lacking specialised expertise (Cartwright, Cartwright, and Edun 2023). Even when professional advice is sought, engagement outcomes are often suboptimal due to content complexity, mismatched communication styles, or fragmented support resources (Khan et al. 2025b; Renaud and Weir 2016). Additionally, the use of fear appeals to encourage adoption remains contested; while intended to motivate protective behaviour, some evidence suggests such approaches may disengage SMEs or reinforce misconceptions, whereas others argue they may be necessary to counter complacency (Bada and Nurse 2019; Renaud and Dupuis 2019).

Taken together, these findings align with broader reviews indicating that SMEs commonly face limited expertise, resource pressures, fragmented guidance, and difficulties translating 'good practice' into actionable implementation (Chidukwani, Zander, and Koutsakis 2022; Junior, Becker, and Johnson 2023). From a behavioural perspective, resource limitations and difficulties accessing or understanding cybersecurity guidance can create an awareness-action gap, where SMEs recognise cyber risks but still struggle to adopt recommended security practices. Consistent with this interpretation, Jamil et al. (2025) show that coping appraisal factors, particularly self-efficacy, response efficacy, and perceived costs, are stronger predictors of secure behaviour than threat susceptibility alone. This suggests that perceived vulnerability is insufficient to drive adoption in the absence of feasible, contextually aligned support. Consequently, a mismatch persists between prevailing engagement approaches and the practical realities under which SMEs operate. The following section therefore examines the limitations of existing engagement approaches.

1.4. Limitations of existing engagement approaches

Much of the existing research and policy literature treats SMEs as a homogeneous group, resulting in generic 'one size fits all' strategies and recommendations that often fail to account for organisational diversity and can be impractical for resource-constrained small-business environments (Chidukwani, Zander, and Koutsakis 2022; Heidt, Gerlach, and Buxmann 2019). This homogenised perspective overlooks critical contextual differences in organisational size, resources, and digital maturity (Junior, Becker, and Johnson 2023), thereby reducing the relevance, uptake, and overall effectiveness of proposed interventions (Khan et al. 2025a).

Recognition of SME heterogeneity has led to attempts at subcategorization to better tailor support. The EU Small Business Standard (SBS) framework, for example, distinguishes between Digitally Dependent firms (reliant on ICT for operations), Digitally Based firms (providers of digital solutions such as websites or software), and Digital Enablers (SMEs offering cybersecurity-related services) (SBS 2020). Despite its conceptual value, relatively few studies have operationalised these categories in empirical research. Shojaifar and Järvinen (2021) proposed a five-part taxonomy ranging from 'cybersecurity abandoned' to 'cybersecurity provider' SMEs, but this classification was largely researcher-defined and only lightly validated. Similarly, Van Haastrecht et al. (2021) developed a socio-technical framework to differentiate cybersecurity support needs, yet their work was entirely literature-based and lacked direct SME input.

More recently, Wilson and McDonald (2025) explored micro-business cybersecurity perspectives and engagement preferences through interviews with Digitally Dependent, Digitally Based, and Digital Enabler groups. Their findings revealed notable differences in risk perceptions, IT practices, engagement preferences, and adoption triggers across subgroups, providing important insights into SME diversity. However, while this work advanced understanding of subgroup differences, it did not systematically translate these insights into a clear user-centered framing for cybersecurity support. As a result, protective guidance that does not adequately account for SMEs' specific contexts and constraints risks misalignment with their everyday operational realities. In considering how to address this issue, the following section examines how user-centered design (UCD) approaches might be adapted to more effectively align cybersecurity support with the lived needs and practices of SMEs.

1.5. Understanding user needs through user-centered design (UCD)

User-centered design (UCD) is an approach that places users' needs, contexts, and experiences at the core of the design process, with the aim of producing systems that are effective, efficient, and satisfying to use (ISO 2019). Formalised in ISO 9241–210 and rooted in Human–Computer Interaction (HCI), UCD emphasises active user involvement to ensure that solutions are grounded in real-world contexts (Radnejad, Sarkar, and Osiyevskyy 2022). Central to this approach is the premise that, without a clear understanding of users' environments, goals, and intended outcomes, valid and meaningful requirements are unlikely to be identified (ISO 2019).

A key step in developing such understanding is the identification of 'user needs' (Lo et al. 2025). In service design literature, user needs are typically conceptualised as the underlying goals, motivations, and desired outcomes users seek to achieve through interaction with a service, rather than the specific features or solutions the service provides (Suhaimi, Walters, and Ward 2024). Expressing findings in terms of user needs therefore serves an important translational function as qualitative research often generates rich but complex insights that are not inherently design-ready. By distilling these insights into clearly articulated user-need statements, dispersed or densely presented knowledge can be reorganised into a coherent and accessible framework that is more readily interpretable and actionable for those designing interventions (Suhaimi, Walters, and Ward 2024). In this sense, a user-needs-led framing translates existing knowledge into the voice of the user, in this case, the micro-business owner, making explicit their goals, constraints, and decision-making realities.

The importance of this translational role becomes clearer when considered alongside the persistent research-practice gap in SME cybersecurity: despite a decade of research identifying barriers to adoption and proposing strategies to address them, uptake of recommended practices remains consistently low. This persistence suggests that the challenge may lie less in identifying additional barriers and more in how existing knowledge is communicated, structured, and translated into practice. A growing body of evidence indicates that SME cybersecurity guidance remains underutilised because it is often presented in formats that are overly complex, insufficiently actionable, or framed as generic solutions that fail to reflect SME contexts (Junior, Becker, and Johnson 2023; Khan et al. 2025a; Saha and Anwar 2024). A user-needs-led framing offers one potential mechanism for narrowing this research-practice gap by rendering knowledge more design-ready, context-sensitive, and aligned with the everyday realities of micro-business decision-makers. To demonstrate the practical relevance of this approach, the following section examines empirical examples of user-needs-led approaches in practice and illustrates how articulated user needs can inform more user-aligned and actionable design.

1.6. Evidence of user needs approaches in practice

User-needs-led approaches are evident across a wide range of academic domains as well as in industry. In healthcare, synthesising user needs from both patients and clinicians has been shown to shift design attention away from technology-led features toward outcome-oriented requirements that reflect real care practices, workflows, and patient priorities, thereby supporting more person-centered service development (Chute et al. 2022). sSimilarly, Rooney and Jelenewicz (2026) demonstrate that translating patients' experiences with medical devices into formalied user-need statements helped designers move beyond surface usability issues, enhancing empathy for users' lived experiences and enabling more contextually grounded design decisions that accounted for physical, emotional, and situational constraints. To increase the impact of government census data, Lowry et al. (2023) found that eliciting user needs from statisticians, researchers, and policy officials revealed misalignments between existing system functionality and users' analytical and decision-making tasks. Articulating these needs informed the redesign of a national data infrastructure service, resulting in improved usability, clearer information pathways, and better-targeted support provision. The grey literature also contains numerous examples of user-needs-led approaches being used in industry to improve service design. For example, Bank of America's 'Keep the Change' programme emerged from research into customers' everyday saving behaviours, which identified unmet needs for low-effort, automated saving mechanisms. Rather than introducing new financial products, these insights were embedded into service design by rounding up transactions and automatically transferring small amounts into savings, which was credited with attracting over 12 million new customers and generating more than $2 billion in savings (Schmieden 2018).

Taken together, these examples demonstrate how translating rich and often fragmented qualitative insights, ranging from patient narratives and clinician workflows to policy-user frustrations and everyday financial habits, into structured user-need statements can transform complex data into a coherent design direction. By clarifying goals, constraints, and desired outcomes, this reframing can make insights more interpretable and actionable for decision-makers and designers. Building on this cross-domain evidence, we now outline how the present study applies a user-needs-led approach within the context of micro-business cybersecurity.

1.7. The present study

Against this backdrop, the present study adopts a user-needs-led approach to reanalyse interview data collected by Wilson and McDonald (2025) with EU-defined

micro-business sub-groups: Digitally Dependent, Digitally Based, and Digital Enablers. Rather than identifying new cybersecurity barriers, the study seeks to translate qualitative insights into explicitly articulated cybersecurity user needs, expressed in the voice of micro-business decision-makers.

There is no single internationally standardised format for expressing user needs (ISO 2019). Given the UK focus of this study, the UK Government Digital Service (GDS) format was selected as a pragmatic and contextually relevant approach. GDS conceptualises user needs as the goals or problems users are trying to achieve, expressed from the user's perspective (DSIT 2025a). Their format of 'As a [type of user], I need [what the user wants to do] so that [why the user wants to do it]' facilitates the synthesis of qualitative insights while maintaining a focus on outcomes rather than predefined solutions.

Expressing needs in this format enables a structured, user-centered representation of micro-business owners' goals, constraints, and decision-making realities, providing a benchmark against which potential solutions can be considered. This approach also supports systematic comparison across micro-business sub-groups, enabling clearer examination of how cybersecurity needs differ across digital contexts. To explore the 'opportunity space' created by identifying these needs, the study then draws on recommendations from the existing literature to consider how the identified needs might be addressed. These literature-informed solutions are design considerations rather than validated interventions, offered to illustrate how a user-needs-led framing can support more targeted and contextually grounded cybersecurity guidance.

Building on this rationale, the study is guided by the following research questions:

RQ1. What cybersecurity user needs do UK micro-businesses identify when these needs are elicited and articulated using a UCD approach?

RQ2. How do these user needs differ across micro-business Digitally Dependent and Digitally based sub-groups, and how do Digital Enabler perspectives contextualize and help interpret these differences?

RQ3. What literature-informed approaches could address the identified user needs?

2. Materials and methods

This section outlines the methodological approach used to elicit user needs through interviews with Digitally Dependent and Digitally Based micro-businesses, as well as Digital Enablers. It provides an overview of the study's participants, procedures, materials, measures, and data analysis. Ethical approval for this study was granted by the University Research Ethics Committee (approval number 007675).

2.1. Participants and recruitment

Thirty participants recruited for this study were evenly distributed across three groups: ten Digitally Dependent (DD), ten Digitally Based (DB), and ten Digital Enablers (DE). DD participants were small and micro-businesses that relied on IT for day-to-day operations but did not have IT as a core business activity. DB participants were small and micro-businesses that delivered products or services through IT to other businesses, without providing dedicated cybersecurity support. DE participants were organisations whose primary role was to support other firms in strengthening their cybersecurity.

Across the Digitally Dependent and Digitally Based groups, interviewees were typically owners, partners, or managers with decision-making responsibility. Participating organisations represented a range of sectors and were predominantly micro-enterprises; however, two Digitally Based organisations fell within the small-business category (11−50 employees), albeit at the lower end of this range. Most participants were based in North East England and Yorkshire, UK. Purposive sampling (Bernard 2017) was used to identify Digitally Dependent and Digitally Based businesses through a brief online screening survey (see Appendix A). DE participants were recruited separately via the UK Cyber Resilience Centres (CRC) network, comprising cyber consultants and experts who specialise in helping businesses improve their cybersecurity, typically through services such as Cyber Essentials certification and related advisory support.

2.2. Question design

Semi-structured interviews were employed to enable flexible, in-depth exploration of the cybersecurity needs, perceptions, and behaviours of small and micro-businesses. The interview schedule was designed using open-ended, exploratory prompts to elicit accounts while allowing participants to introduce issues most relevant to their organisational context. This generative approach is consistent with qualitative research aiming to capture decision-making processes and lived experiences in complex socio-technical settings (Braun and Clarke 2013).

To ensure that the interview prompts were not only exploratory but also theoretically informed, their design was guided by prior cybersecurity behavioural research that draws on preventative health frameworks to explain

the adoption of protective behaviours among home users, employees, and business decision-makers. Such frameworks seem appropriate in cybersecurity contexts because, like preventative healthcare, cybersecurity involves proactive behaviours intended to mitigate potential future harm rather than respond to immediate incidents. Among these frameworks, Protection Motivation Theory (PMT) (Rogers 1975) and the Health Belief Model (HBM) (Rosenstock 1974) are prominent in cybersecurity research, where they have been widely applied to examine risk perception, protective behaviours, and the adoption of security measures. Although PMT and HBM share conceptual similarities, such as perceived vulnerability, perceived severity, and response efficacy, this study drew primarily on constructs derived from the HBM to inform the interview design. HBM was selected as the principal theoretical scaffold because its construct of cues to action offered a useful lens for discussing participants' triggers that prompted cybersecurity adoption. Importantly, the selection of HBM is not meant to imply that it is more suitable than PMT for explaining cybersecurity behaviour, nor is this study designed to test or validate HBM as a predictive model. Rather, the framework was used to structure and sensitise the interview prompts, ensuring conceptual coherence and alignment with established literature while preserving the inductive nature of the analysis. In this sense, HBM functioned as a conceptual lens rather than a framework for generating and testing formal hypotheses.

Table 1 outlines how the interview questions were mapped to key HBM constructs (e.g. perceived susceptibility, perceived severity, perceived barriers, self-efficacy, and cues to action), while remaining sufficiently open-ended to support inductive theme development. The interview schedule also included additional non-HBM inspired questions to capture SME cybersecurity engagement preferences, the influence of external news reporting and participants' recommendations for improving cybersecurity support for small and micro-businesses.

Interview questions were piloted with cybersecurity professionals, SME owners, and academics to ensure accuracy, clarity, and neutrality. Interviews followed core topics with flexible sub-questions, using laddering to probe simple responses and reveal underlying motivations. Given the well-documented challenges of recruiting SMEs in cybersecurity research (e.g. Osborn and Simpson 2018), interviews were intentionally designed to be concise (approximately 20–30 min) to minimise participant burden and support engagement. To mitigate potential limitations associated with shorter interviews, the interview guide followed best-practice recommendations for semi-structured interviews of limited duration (McGrath, Palmgren, and Liljedahl 2019; Zavattaro and Gille 2026). These recommendations include pilot testing, a focused set of core questions, the use of pre-prepared probes, and careful time management, all of which are intended to maximise the depth and quality of information gathered within shorter interview formats.

2.3. Procedure

Interviews were conducted via video conferencing software, without incentives, and lasted around 20 min. Each session began with brief introductions to build rapport, moved into the main questions guided by the interview protocol but kept flexible to allow natural conversation, and concluded with a short wrap up outlining next steps and giving participants the opportunity to ask questions. Video conferencing software was used to record the interviews and generate draft word transcripts. These were checked against the audio to ensure

Table 1. Interview themes and question areas.

Construct / Theme	Questions	Group(s)	Source
Perceived Vulnerability	How vulnerable do you believe your business/SMEs are to cyber-attacks? Do you think SMEs are as vulnerable as larger organisations?	DD, DB, DE	Claar (2011)
	Do SMEs deliberately leave themselves vulnerable?	DE	Self-developed
	What do you understand by the term 'hacking'?	DD, DB	Self-developed
Perceived Severity	If your business/SMEs were hacked, what might the impacts be?	DD, DB	Claar (2011)
Perceived Benefits	What do you/SMEs see as the return on investing in cybersecurity?	DD, DB, DE	Ng, Kankanhalli, and Xu (2009)
Perceived Barriers	What prevents you/SMEs from investing in cybersecurity?	DD, DB, DE	Ng, Kankanhalli, and Xu (2009)
Self-Efficacy	How do you/SMEs maintain cybersecurity?	DD, DB, DE	Ng, Kankanhalli, and Xu (2009)
Cues to Action	What motivates you/SMEs to adopt cybersecurity?	DD, DB, DE	Osborn and Simpson (2018)
Engagement	What do SMEs usually ask you for help with?	DE	Self-developed
	How do you currently receive cybersecurity guidance, and how would you prefer to receive it?	DD, DB	Self-developed
Influencers	How do news stories about cyber-attacks influence your security practices?	DD, DB	Self-developed
Improvements	What could improve the future of SME cybersecurity?	DD, DB, DE	Self-developed

DD = *D*igitally Dependent; DB = Digitally Based; DE = Digital Enabler.
Note: Table 1 is adapted with modifications from Wilson and McDonald (2025).

verbatim accuracy. To maintain anonymity, identifiers were removed and participants were assigned pseudonyms (DD, DB, DE) and numerical codes (1–10).

2.4. Data analysis

Word transcripts were subjected to thematic analysis in Atlas.ti 25 using an inductive open-coding approach conducted by the first author. While the interview guide was theory-informed (HBM), analysis was conducted inductively and was not structured around HBM constructs. The purpose was to identify quotations that explicitly or implicitly addressed participants' cybersecurity needs, challenges, or preferences. Quotations were retained when they provided substantive insights, such as articulating participants' perspectives, rationales for their decisions, or the underlying reasons for their needs, challenges, or expectations. Implicit statements, where perspectives could be inferred rather than directly stated, were also included. Text segments that did not contribute relevant insights into user needs were excluded. For Digital Enablers, quotations were retained when they reflected perceptions or experiences of small businesses' cybersecurity needs, challenges, or preferences. Although Digital Enabler input was analysed alongside micro-business data, it reflects their experiences of working with SMEs rather than the SMEs' own perspectives. Accordingly, these insights were used to triangulate findings and provide contextual understanding, not to replace the views of Digitally Dependent or Digitally Based businesses. This process yielded a grand total of **446 quotations**.

2.4.1. Code development

The 446 quotations were subsequently coded by the first author, through an iterative process in which quotations of similar meaning were grouped together. Groups were assigned labels that drew on words or phrases used within the quotations themselves. The intent was to ensure conceptual coherence, with all quotations assigned to a group and none excluded. Through iterative refinement, the groups were consolidated into broader thematic categories, which constituted the major codes of the analysis:

Cybersecurity Guidance – Participants' needs for protective guidance, including desired content, forms of support, and expectations of cybersecurity experts (224 quotations).

Cybersecurity Posture – Participants' needs relating to the assessment of current cybersecurity practices, threats, and risk management, with emphasis on present activities and requirements (99 quotations).

Resources – Needs concerning time, finances, and expertise, as well as the ways in which resource limitations contributed to the deprioritization of cybersecurity in favour of competing demands (39 quotations).

Return on Investment (ROI) – Needs associated with understanding, or difficulties in discerning, the return on investment from cybersecurity measures (84 quotations).

2.4.2. Sub-Code development

Each major code was further refined into sub-codes by the first author, enabling the identification of narrower but conceptually related categories. The refinement process was conducted iteratively until thematic saturation was achieved. High-frequency sub-codes were further disaggregated, whereas low-frequency sub-codes were either merged or retained as stand-alone categories. This process ultimately yielded a comprehensive set of **36 sub-codes**. A codebook was subsequently developed to document the definition, scope, and application criteria of each code and sub-code (Appendix B).

2.5. Intercoder reliability

Intercoder reliability was used to evaluate the consistency with which the first and fourth authors interpreted and applied the codebook. Reliability was assessed at the theme level. To facilitate this process, interview data were exported to Atlas.ti 25 as a project containing pre-defined quotations without assigned code labels. The fourth author independently coded a pilot sample of nine randomly selected interview transcripts (three from each DD, DB, and DE participant group) using the developed codebook. Intercoder agreement for the pilot yielded a Krippendorff's alpha of $\alpha = 0.72$. Consistent with iterative qualitative coding practices (Halpin 2024), the authors met to review coding discrepancies, which primarily arose in the differentiation and allocation between Guidance and Posture codes. These discrepancies were resolved through discussion and minor codebook clarification before proceeding to full double-coding of all 30 transcripts, resulting in an improved Krippendorff's alpha of $\alpha = 0.84$, indicating strong intercoder reliability and consistent application of the coding framework (Krippendorff 2004).

2.6. Presentation of user needs

User needs were derived by systematically translating sub-codes and their quotations into statements using the Government Digital Service (GDS) format (GOV.UK 2017):

> As a [type of user], I need [what the user wants to do] so that [why the user wants to do it].

The process followed three steps. First, the type of user was specified (here, micro-businesses). Second, the user's goal (what the user wants to do) was considered by identifying the overall needs, wants, and desires expressed by the quotations contained within a sub-code. Third, the underlying rationale (the why) was articulated by examining the sub-codes' quotations for clues as to why the goal was important. Once the 36 draft statements were produced, they underwent validation to ensure conceptual clarity, distinctiveness, and representativeness of the underlying data.

2.6.1. Validation

Draft user needs were validated against the Government Digital Service (GDS) criteria. This process involved systematically assessing each need to ensure that it:

- Reflected the authentic voice of small business owners (i.e. it reads like something a real owner would say).
- Prioritised the articulation of problems rather than solutions.
- Was concise, descriptive, and transparent regarding user motivations.
- Was stable over time and unlikely to undergo substantive change.
- Was actionable for stakeholders engaged in small business cybersecurity.

Conversely, users' needs were rejected or revised if they:

- Presupposed a specific solution, feature, or technology.
- Were framed in terms too broad to permit meaningful interpretation.
- Were excessively narrow, thereby precluding alternative possibilities.

2.6.2. Worked example

For transparency, the following illustrates how an interview excerpt was translated into a GDS-style user need by applying the three-step process and subsequent GDS validation.

Interview Quotation: *Nothing stood out enough to make me think this is clear, easy and obvious as to what they're trying to get to and what would make sense as to what steps to take.*

Code and Sub-Code

- Code: Guidance – the quotation concerns needs related to protective guidance received.
- Sub-code: Actionable – the quotation highlights a need for guidance that clearly specifies steps to take.

Three-Step Translation Process

(1) Specify the type of user: The type of user is specified as micro-businesses (here operationalised in the statement *as a micro-business owner*).
(2) Identify the user's goal (the 'what'): From the quotation, the central goal is to receive guidance that translates into clear, concrete steps.
    What = *cybersecurity guidance I can act on.*
(3) Articulate the underlying rationale (the 'why'): The quotation implies frustration with ambiguity and a desire to know what to do next.
    Why = *so that I can actually do something with it.*

Resulting GDS-style user need: As a micro-business owner, I need cybersecurity guidance that I can act on so that I can actually do something with it.

Validation Against GDS Criteria of the Example

The statement retains the user's voice, frames a clear problem/goal *(guidance I can act on)* without naming a solution *(e.g. no specific format or channel)*, is concise and actionable, and is likely to remain stable across contexts where clarity of next steps is important.

Using this procedure, we produced 36 distinct user needs, each directly linked to a unique parent sub-code, which are presented in the Results section.

3. Results

The results are presented in two stages: first, interviewee demographics and responses to the screening survey on current IT use are described; second, user needs are reported – organised by codes and sub-codes.

3.1. Interviewee demographics

Table 2 summarises the demographic characteristics of interviewees, collected through a brief pre-interview survey.

3.2. Screener survey

Table 3 outlines IT management approaches, current practices, types of data processed, and prior incidents of victimisation among Digitally Based and Digitally Dependent groups.

Table 2. Summarises the demographic characteristics of interviewees, collected through a brief pre-interview survey.

Demographic factor	Digitally dependent (n = 10)	Digitally based (n = 10)	Digital enablers (n = 10)
Company Size	Micro (10)	Micro (8), Small (2)	N/A
Respondent's Position	Owner/Partner (7), Management (3)	Owner/Partner (10)	Owner/Partner (7), Management (3)
Region	NE & Yorkshire (9), East Midlands (1)	NE & Yorkshire (9), Southwest (1)	NE & Yorkshire (10)
Business Sector	Food & Hospitality (1), Media (2), Charity (2), Retail/ Wholesale (2), Events (1), Consultancy (1), Construction (1)	Retail/Wholesale (1), Recruitment (2), Software Development (6), Social Media (1)	Cybersecurity Consultancy (10)
Business Age	Mean = 9.1 yrs, Median = 4.5, Range = 45	Mean = 11.5 yrs, Median = 8, Range = 43	N/A
SMEs Worked With (Security)	N/A	N/A	Mean = 862, Median = 175, Range = 4,890

Note: Table 2 is adapted with modifications from Wilson and McDonald (2025).

Table 3. IT practices of digitally dependent and digitally based SMEs.

IT practice	Digitally dependent (n = 10)	Digitally based (n = 10)
How IT is managed	DIY (6), In-house member (1), Outsourced (3)	DIY (1), In-house member (4), In-house IT personnel (1), Outsourced (4)
Devices (number)	Mean = 8.2, Median = 4.5, Mode = 2, Range = 23	Mean = 14.8, Median = 10, Mode = 6, Range = 45
Logging	No (10)	No (8), Yes (2)
*Store/Process PII	Yes (6), No (4)	Yes (8), No (2)
Victim of incident	Yes (1), No (9)	Yes (2), No (8)

* PII = Personally Identifiable Information e.g. names, addresses, email addresses, phone numbers, or financial details.
Note: Table 3 is adapted with modifications from Wilson and McDonald (2025).

3.3. Thematic analysis

User needs are organised alphabetically at both the code and sub-code levels. Findings are reported using Code Counts (CC), Sub-Code Counts (SCC), and Interviewee Counts (IC) to capture both the volume of data associated with each need and the extent to which these needs are shared across participants. IC percentages (IC%) indicate the proportion of interviewees who mentioned each need. These are calculated within each subgroup ($n = 10$) and across the full sample ($n = 30$), enabling comparison of how prevalent different needs are among Digitally Dependent (DD) and Digitally Based (DB) participants, alongside perspectives from Digital Enablers (DEs) based on their experience supporting SMEs. IC values reflect the number of unique participants who mention a need, rather than the frequency of quotations. IC% is calculated using participant totals ($n = 10$ per subgroup; $n = 30$ overall). Table 4 summarises this analytical approach.

3.3.1. Code analysis

Table 5 presents the code-level analysis of interviews, identifying four broad thematic areas of user needs.

Cybersecurity Guidance accounted for the highest code and interviewee counts, indicating our sample's heavy reliance on external expertise to navigate cybersecurity. This prominence suggests that Guidance is a foundational need, enabling small businesses to subsequently assess their security posture, evaluate ROI, and allocate resources. Other themes appear secondary, reflecting how practical advice underpins SMEs' ability to engage with more strategic considerations. Tables 6–10 provide direct answers to RQ1 based on micro-business participants (DD and DB), while also enabling interpretation alongside Digital Enabler perspectives. Interviewee-count (IC) cells outlined in black denote cases of group incongruence (≥ 4 interviewees), a threshold chosen to highlight meaningful differences while reducing the risk of overinterpreting smaller interview counts. Together, these findings show how needs differ between Digitally Dependent and Digitally Based micro-businesses.

3.3.2. Sub-Code analysis: cybersecurity guidance

Tables 6 and 7 present the sub-codes contained within the cybersecurity Guidance category, listing 17 user needs, presented in alphabetical order.

Taken together, the results suggest that most Guidance needs in Tables 6 and 7 were widely reported by Digitally Dependent and Digitally Based participants, with similar patterns reflected in Digital Enabler perspectives. However, some notable differences emerged. Digital Enablers ($n = 6$), drawing on their consultancy experience, highlighted the need to *bring threats to life* more frequently than Digitally Dependent participants ($n = 2$). A similar pattern was observed for the need to understand the *right amount to spend*, where DE perspectives ($n = 5$) emphasised this more than Digitally Dependent participants ($n = 1$). In addition, Digitally Dependent participants ($n = 6$) expressed a stronger desire for *guidance to reach them automatically* than Digitally Based participants ($n = 1$), with comparatively lower emphasis observed in DE perspectives ($n = 2$).

Table 4. Presentation of user needs at the code and sub-code levels.

Code	Description	Group	Code Count (CC)	Interviewee Count (IC)	IC Proportion (IC%)
Descriptive name of Code	Description of user needs captured within the code	DD	Individual count	Individual count	IC ÷ 10 × 100
		DB	Individual count	Individual count	IC ÷ 10 × 100
		DE	Individual count	Individual count	IC ÷ 10 × 100
		Total	Cumulative CC count of all groups	Cumulative IC count of all groups	IC ÷ 30 × 100
Sub Code	User Need	Group	Sub-Code Count (SCC)	Interviewee Count (IC)	IC Proportion (IC%)
Descriptive name of Sub Code	User need associated with the sub-code, presented in GDS format	DD	Individual count	Individual count	IC ÷ 10 × 100
		DB	Individual count	Individual count	IC ÷ 10 × 100
		DE	Individual count	Individual count	IC ÷ 10 × 100
		Total	Cumulative SCC count of all groups	Cumulative IC count of all groups	IC ÷ 30 × 100

Code Count (CC) = Total number of quotes assigned to a code.
Sub Code Count (SCC) = Total number of quotes assigned to a sub-code.
Interviewee Count (IC) = Number of unique interviewees who mentioned the code/sub-code.
IC Proportion (IC%) = Proportion of interviewees who mentioned a code or sub-code; calculated within each subgroup (IC ÷ 10 × 100) and across the full sample (IC ÷ 30 × 100).
DD = Digitally Dependent.
DB = Digitally Based.
DE = Digital Enabler.
Total = Combined counts across DD, DB, and DE groups.
Note: Values for DD and DB represent direct expressions of user needs reported by micro-business participants. Values for DE reflect provider perspectives based on experience working with SMEs and are included to help interpret and support the findings, rather than as direct expressions of user needs.

Table 5. Code-level analysis of interviews, showing four overarching thematic areas of user needs DD/DB = direct user needs; DE = provider perspectives for contextualisation.

Code	Description	Group	CC	IC	IC%
Cybersecurity Guidance	Interviewees' needs related to protective guidance - what they want included, the help they require, and what they expect from cyber experts	DD	66	10	100
		DB	68	10	100
		DE	90	10	100
		Total	224	30	100
Cybersecurity Posture	Interviewees' needs in assessing their current cybersecurity from threat, protection, and risk perspectives - focused on what they are doing and need now	DD	38	9	90
		DB	24	8	80
		DE	10	9	90
		Total	99	26	87
Resource	Interviewees' resource needs (time, money, and expertise), and how limited resources precipitate the deprioritisation of cybersecurity in favour of competing demands	DD	16	6	60
		DB	10	5	50
		DE	13	7	70
		Total	39	18	60
Return on Investment (ROI)	Interviewees cybersecurity ROI (Return on Investment) needs (or difficulty in being to discern cybersecurity ROI)	DD	16	9	90
		DB	38	10	100
		DE	30	10	100
		Total	84	29	97
	Grand Total	DD	136	34	
	Grand Total	DB	140	33	
	Grand Total	DE	143	36	
	Grand Total	Total	446	103	

Table 8 now presents the sub-code analysis of the cybersecurity posture theme.

3.3.3. Sub-Code analysis: cybersecurity posture

Taken together, the results in Table 8 indicate that most posture-related needs were broadly consistent across Digitally Dependent and Digitally Based participants, with similar patterns reflected in Digital Enabler perspectives. The only notable difference was in *Governance*, where Digital Enablers ($n = 7$), drawing on their experience supporting SMEs, emphasised that, in their view, SMEs need support in understanding which cybersecurity regulations and compliance requirements apply to them, compared with Digitally Based ($n = 2$) and Digitally Dependent ($n = 0$) participants.

Table 9 presents the sub-code analysis of the cybersecurity resource theme.

3.3.4. Sub-Code analysis: cybersecurity resource

No areas of incongruence were identified within the resource-related needs, indicating broad agreement across Digitally Dependent and Digitally Based

Table 6. Sub-code analysis of the Cybersecurity Guidance theme (first nine user needs).

Sub-code	User need	Group	SCC	IC	IC%
Actionable	As a micro business owner, I need cybersecurity guidance I can act on, so that I can actually do something with it	DD	0	0	0.0
		DB	3	2	20.0
		DE	1	1	10.0
		Total	4	3	10.0
Bite Sized	As a micro business owner, I need bite-sized chunks of information, so that its easier for me to digest	DD	2	2	20.0
		DB	0	0	0.0
		DE	1	1	10.0
		Total	3	3	10.0
Bring Threats to Life	As a micro business owner, I need to see threats in action, so that I can understand them better	DD	3	2	20.0
		DB	4	3	30.0
		DE	9	6	60.0
		Total	16	11	36.7
Comparisons	As a micro business owner, I need to be able to compare different cybersecurity products, so that I can decide which is best for me	DD	2	2	20.0
		DB	5	3	30.0
		DE	0	0	0.0
		Total	7	5	16.6
Engaging	As a micro business owner, I need cybersecurity guidance that's interesting so that I don't switch off.	DD	2	2	20.0
		DB	4	4	40.0
		DE	2	2	20.0
		Total	8	8	26.7
Finding Help	As a micro business owner, I need help finding cybersecurity support, so that I can be sure I'm speaking to the right people	DD	5	5	50.0
		DB	8	6	60.0
		DE	7	4	40.0
		Total	20	15	50.0
List	As a micro business owner, I need a list of actions I should take, so that I know what I need to do to keep my business safe	DD	2	2	20.0
		DB	6	3	30.0
		DE	1	1	10.0
		Total	9	6	20.0
Longevity	As a micro business owner, I need regular, ongoing support, so that I have someone I can turn to whenever I need help	DD	1	1	10.0
		DB	1	1	10.0
		DE	4	4	40.0
		Total	6	6	20.0
No Fear Uncertainty or Doubt	As a micro business owner, I need cybersecurity guidance that doesn't scare me, so that I worry less	DD	1	1	10.0
		DB	2	1	10.0
		DE	5	4	40.0
		Total	8	6	20.0
No Hard Sell	As a micro business owner, I need cybersecurity sales without the hard sell, so that I know I'm not just being sold to hit a target	DD	1	1	10.0
		DB	1	1	10.0
		DE	4	3	30.0
		Total	6	5	16.6
Reach Me	As a micro business owner, I need cybersecurity advice to reach me so that I don't waste my time looking for it	DD	6	6	60.0
		DB	2	1	10.0
		DE	3	2	20.0
		Total	11	9	30.0
Right Amount To Spend	As a micro business owner, I need to know how much I should spend on cybersecurity, so that I'm investing the right amount to stay safe	DD	1	1	10.0
		DB	2	2	20.0
		DE	5	5	50.0
		Total	8	8	26.7
Scale Up Actions	As a micro business owner, I need to know what actions I should take if my business expands, so that I can keep it safe	DD	3	2	20.0
		DB	0	0	0.0
		DE	1	1	10.0
		Total	4	3	10.0
Simple	As a micro business owner, I need jargon-free cybersecurity help, so that I can understand it	DD	5	3	30.0
		DB	5	3	30.0
		DE	6	2	20.0
		Total	16	8	26.7
Tailored	As a micro business owner, I need advice that's tailored to my business, so that I know I'm doing the right things to protect it	DD	7	5	60.0
		DB	4	3	30.0
		DE	12	4	40.0
		Total	23	12	40.0
Trust Source	As a micro business owner, I need to trust the advice I receive, so that I know it's in my best interests	DD	12	7	23.3
		DB	14	9	30.0
		DE	17	7	23.3
		Total	43	23	76.7
Understanding What To Prioritize	As a micro business owner, I need to know, out of all the things I could do, what I should do, so that I know I'm doing the right things	DD	13	7	70.0
		DB	7	4	40.0
		DE	12	6	60.0
		Total	32	17	56.7
		DD	66	49	
		DB	68	46	
		DE	90	53	
		Total	224	148	

(*Continued*)

Table 6. Continued.

Sub-code	User need	Group	SCC	IC	IC%
No Hard Sell	As a micro business owner, I need cybersecurity sales without the hard sell, so that I know I'm not just being sold to hit a target	DD	1	1	10.0
		DB	1	1	10.0
		DE	4	3	30.0
		Total	6	5	16.6
Reach Me	As a micro business owner, I need cybersecurity advice to reach me so that I don't waste my time looking for it	DD	6	6	60.0
		DB	2	1	10.0
		DE	3	2	20.0
		Total	11	9	30.0
Right Amount To Spend	As a micro business owner, I need to know how much I should spend on cybersecurity, so that I'm investing the right amount to stay safe	DD	1	1	10.0
		DB	2	2	20.0
		DE	5	5	50.0
		Total	8	8	26.7
Scale Up Actions	As a micro business owner, I need to know what actions I should take if my business expands, so that I can keep it safe	DD	3	2	20.0
		DB	0	0	0.0
		DE	1	1	10.0
		Total	4	3	10.0
Simple	As a micro business owner, I need jargon-free cybersecurity help, so that I can understand it	DD	5	3	30.0
		DB	5	3	30.0
		DE	6	2	20.0
		Total	16	8	26.7
Tailored	As a micro business owner, I need advice that's tailored to my business, so that I know I'm doing the right things to protect it	DD	7	5	60.0
		DB	4	3	30.0
		DE	12	4	40.0
		Total	23	12	40.0
Trust Source	As a micro business owner, I need to trust the advice I receive, so that I know it's in my best interests	DD	12	7	23.3
		DB	14	9	30.0
		DE	17	7	23.3
		Total	43	23	76.7
Understanding What To Prioritize	As a micro business owner, I need to know, out of all the things I could do, what I should do, so that I know I'm doing the right things	DD	13	7	70.0
		DB	7	4	40.0
		DE	12	6	60.0
		Total	32	17	56.7

DD/DB = direct user needs; DE = provider perspectives for contextualisation.

participants, with consistent patterns reflected in Digital Enabler perspectives. This suggests that challenges relating to time, money, expertise, and resource allocation are widely shared among micro-businesses, regardless of their digital orientation.

Next, Table 10 presents the final sub-code analysis, focusing on the cybersecurity return on investment (ROI) theme.

3.3.5. Sub-Code analysis: cybersecurity ROI

Three notable differences emerged from the incongruence analysis of ROI-related needs. First, the need for cybersecurity to mitigate reputational damage from a cyberattack was emphasised far more frequently by Digitally Based interviewees ($n = 9$) than by Digitally Dependent ($n = 1$) or Digital Enabler ($n = 4$) perspectives. Second, the need for cybersecurity to protect the business from harm showed incongruence, with Digitally Dependent interviewees ($n = 5$) differing from Digitally Based ($n = 1$), while Digital Enabler perspectives ($n = 3$) reflected patterns similar to the Digitally Based group. Finally, Digital Enablers ($n = 5$), drawing on their experience supporting SMEs, highlighted cybersecurity as a source of competitive advantage, arguing that strong cybersecurity could differentiate a business and help win clients, whereas only one participant from each of the Digitally Dependent and Digitally Based groups mentioned this.

Table 11 summarises sub-code user-need incongruences (any group interviewee counts ≥ 4), showing each sub-code's proportion within its parent code category and pairwise agreement (✓) or disagreement (✗) between Digitally Dependent (DD), Digitally Based (DB) groups, and Digital Enabler (DE) perspectives.

While Guidance contained the largest number of needs overall ($n = 17$), only 18% were incongruent. Posture displayed even fewer divergences (10%). In contrast, ROI stands out, with 60% ($n = 3$) of its needs identified as incongruent – suggesting that ROI considerations are more contested than the Guidance or Governance codes.

This concludes the results section. The following discussion situates these findings within the existing literature and offers recommendations for addressing the identified needs.

4. Discussion

This discussion proceeds in three parts. We begin by analysing the user needs identified in the study (RQ1) in relation to the extant literature, then consider how

Table 7. Sub-code analysis of the Cybersecurity Guidance theme (remaining eight user needs) DD/DB = direct user needs; DE = provider perspectives for contextualisation.

Sub-code	User need	Group	SCC	IC	IC%
No Hard Sell	As a micro business owner, I need cybersecurity sales without the hard sell, so that I know I'm not just being sold to hit a target	DD	1	1	10.0
		DB	1	1	10.0
		DE	4	3	30.0
		Total	6	5	16.6
Reach Me	As a micro business owner, I need cybersecurity advice to reach me so that I don't waste my time looking for it	DD	6	6	60.0
		DB	2	1	10.0
		DE	3	2	20.0
		Total	11	9	30.0
Right Amount To Spend	As a micro business owner, I need to know how much I should spend on cybersecurity, so that I'm investing the right amount to stay safe	DD	1	1	10.0
		DB	2	2	20.0
		DE	5	5	50.0
		Total	8	8	26.7
Scale Up Actions	As a micro business owner, I need to know what actions I should take if my business expands, so that I can keep it safe	DD	3	2	20.0
		DB	0	0	0.0
		DE	1	1	10.0
		Total	4	3	10.0
Simple	As a micro business owner, I need jargon-free cybersecurity help, so that I can understand it	DD	5	3	30.0
		DB	5	3	30.0
		DE	6	2	20.0
		Total	16	8	26.7
Tailored	As a micro business owner, I need advice that's tailored to my business, so that I know I'm doing the right things to protect it	DD	7	5	60.0
		DB	4	3	30.0
		DE	12	4	40.0
		Total	23	12	40.0
Trust Source	As a micro business owner, I need to trust the advice I receive, so that I know it's in my best interests	DD	12	7	23.3
		DB	14	9	30.0
		DE	17	7	23.3
		Total	43	23	76.7
Understanding What To Prioritise	As a micro business owner, I need to know, out of all the things I could do, what I should do, so that I know I'm doing the right things	DD	13	7	70.0
		DB	7	4	40.0
		DE	12	6	60.0
		Total	32	17	56.7

the literature helps explain differences in needs across micro-business contexts (RQ2), and finally draw on the literature to explore design-oriented approaches for addressing these needs (RQ3).

4.1. RQ1. What cybersecurity user needs do UK micro-businesses identify when these needs are elicited and articulated using a UCD approach?

At the code level, our findings reveal four overarching categories of need: Guidance, Posture, Resources, and Return on Investment (ROI). Cybersecurity Guidance emerged as the most prominent category, both in sub-code and interviewee counts. This suggests that micro-businesses' most pressing needs centre on receiving clear and context-specific advice that they can feasibly act upon, reflecting their constrained in-house cybersecurity capabilities. This interpretation aligns with the literature review by Saha and Anwar (2024), which highlights the need for tailored, entrepreneur-focused cybersecurity guidance that reflects the contextual realities of small businesses. As Khan et al. (2025b) note, in the absence of such guidance SMEs often rely heavily on external experts to interpret risks and translate technical recommendations into practical decisions. This reliance can be problematic for micro-businesses, many of which lack access to such expertise due to cost constraints (Alahmari and Duncan 2020) or uncertainty about where to obtain appropriate support (Renaud and Ophoff 2021).

Importantly, the prominence of Guidance needs appears to reflect not simply a deficit of information, but a deficit of *usable* information. Participants repeatedly emphasised the need to know what to prioritise and to receive guidance that is clear, concise, and easy to locate. This aligns with principles in user-centered design research, which emphasise that the way information is structured and presented can either reduce or increase the cognitive effort required for users to act (ISO 2019). It may be that our micro-business participants are not necessarily seeking more cybersecurity information; rather, they are seeking support that

Table 8. Sub-code analysis of the Cybersecurity Posture theme, listing 10 user needs DD/DB = direct user needs; DE = provider perspectives for contextualisation.

Sub-code	User need	Group	SCC	IC	IC%
Assessing IT Suppliers Competence	As a micro business owner, I need to know if my IT suppliers are up to scratch, so that they are keeping my business safe	DD	5	1	10
		DB	2	2	20
		DE	3	3	30
		Total	10	6	20
Boundaries	As a micro business owner, I need to know where my responsibilities end and my supplier's begin, so that everything is covered	DD	2	1	10
		DB	0	0	0
		DE	0	0	0
		Total	2	1	3.3
Doesn't Hinder	As a micro business owner, I want cybersecurity that doesn't make it hard for me to use my IT so that I'm not slowed down.	DD	0	0	0
		DB	2	1	10
		DE	0	0	0
		Total	2	1	3.3
Governance	As a micro business owner, I need to know what cybersecurity rules apply to me, so that I can follow them	DD	0	0	0
		DB	2	2	20
		DE	10	7	70
		Total	12	9	30
Hackers	As a micro business owner, I need to know how and why hackers might attack me, so that I can figure out if they are a threat	DD	18	6	60
		DB	5	5	50
		DE	3	3	30
		Total	26	14	46.7
Identifying My Threats	As a micro business owner, I need to know what threats I am likely to face so that I can put things into place to stop them	DD	2	2	20
		DB	1	1	10
		DE	6	3	30
		Total	9	6	20
Identifying My Weaknesses	As a micro business owner, I need to know what my cybersecurity weaknesses are, so that I can improve them	DD	5	4	40
		DB	2	2	20
		DE	8	4	40
		Total	15	10	33.3
Monitoring	As a micro business owner, I need someone to watch my IT 24/7, so that I'm constantly covered	DD	0	0	0
		DB	2	1	10
		DE	0	0	0
		Total	2	1	3.3
News Relevancy	As a micro business owner, I need to know if cyber-attack news reports are relevant to me, so that I can figure out if I need to do something	DD	2	2	20
		DB	1	1	10
		DE	1	1	10
		Total	4	4	13.3
Quantifying Risk	As a micro business owner, I need to know the likelihood of my business being attacked, so that I can justify spending my money on security	DD	4	4	40
		DB	4	4	40
		DE	9	5	50
		Total	17	13	43.3
		DD	38	20	
		DB	21	19	
		DE	40	26	
		Total	99	65	

reduces their 'translation work' required to convert abstract or complex recommendations into prioritised, concrete actions within time – and resource-constrained environments. From a behavioural perspective, this emphasis on prioritisation, clarity, and feasibility reflects the importance of lowering perceived response costs while strengthening self-efficacy. The Health Belief Model (HBM) and Protection Motivation Theory (PMT) suggest that effort, complexity, and inconvenience can deter protective behaviour, whereas coping appraisal, particularly confidence in one's ability to act, encourages adoption (Barlette, Gundolf, and Jaouen 2017; Jamil et al. 2025). In this sense, Guidance functions not merely as information provision, but as an enabling mechanism that makes protective action 'low effort to interpret' and practically achievable.

By comparison, needs relating to Posture, ROI, and Resources were mentioned less frequently. While still important, these appear secondary, perhaps because businesses require a baseline of structured guidance before they can meaningfully assess their posture, justify ROI, or allocate resources effectively. Guidance therefore operates as a gateway enabler: without clear direction on what matters and what to do first, risk awareness alone is unlikely to translate into protective action.

Turning to the sub-code findings, Tables 12–15 situate the results within the existing literature, indicating where they confirm prior work and where they extend current understanding of micro-business cybersecurity needs. For those needs that extend prior research, additional discussion is provided beneath each table to explore their contributions and practical implications.

Table 9. Sub-code analysis of the cybersecurity resource theme, listing 4 user needs DD/DB = direct user needs; DE = provider perspectives for contextualisation.

Sub-code	User need	Group	SCC	IC	IC%
Allocating Resource	As a micro business owner, I need to understand why cybersecurity should come before other demands, so that I can decide if it's more important than the rest.	DD	2	2	20
		DB	3	2	20
		DE	2	2	20
		Total	7	6	20
Expertise	As a micro business owner, I need access to people who understand cybersecurity, so that I can tap into their knowledge	DD	3	3	30
		DB	0	0	0
		DE	3	2	20
		Total	6	5	16.7
Money	As a micro business owner, I need more money so that I can afford to pay for cybersecurity	DD	3	2	20
		DB	5	3	30
		DE	5	4	40
		Total	13	9	30
Time	As a micro business owner, I need to more time so that I have the space to do cybersecurity	DD	8	5	50
		DB	2	2	20
		DE	3	2	20
		Total	13	9	30
		DD	16	12	
		DB	10	7	
		DE	13	10	
		Total	39	29	

Table 10. Sub-code analysis of the cybersecurity ROI theme, listing 5 user needs DD/DB = direct user needs; DE = provider perspectives for contextualisation.

Sub-code	User need	Group	SCC	IC	IC%
Alleviate Worry	As a micro business owner, I need my investment in cybersecurity to reduce my worry, so that I feel less worried about attacks	DD	9	7	70
		DB	6	5	50
		DE	5	4	40
		Total	20	16	53.3
Determining ROI	As a micro business owner, I need to be able to determine what the return on my cybersecurity investments are, so that I know I'm getting value	DD	4	4	40
		DB	6	3	30
		DE	7	6	60
		Total	17	13	43.3
Reputation	As a micro business owner, I need my investment in cybersecurity to protect my reputation, so that my clients don't leave me	DD	1	1	10
		DB	16	9	90
		DE	6	4	40
		Total	23	14	46.7
Safer	As a micro business owner, I need my cybersecurity investment to protect my business, so that I don't become a victim	DD	1	1	10
		DB	8	5	50
		DE	3	3	30
		Total	12	9	30
Winning Business	As a micro business owner, I need my cybersecurity investment to be stronger than my competitors', so it helps me win business	DD	1	1	10
		DB	2	1	10
		DE	9	5	50
		Total	12	7	23.3
		DD	16	14	
		DB	38	23	
		DE	30	22	
		Total	84	59	

4.1.1. Cybersecurity guidance need

The extant literature highlights the value of using analogies, metaphors, and narratives in making abstract risks more relatable (Haney and Lutters 2018). The user need, "I need to see threats in action so that I can understand them better," further extends this area of understand ing by indicating that, for many micro-businesses, effective comprehension requires not only simplified explanations or analogies, but also opportunities to observe how cyber threats manifest in practice. Visualisation – through live demonstrations or tangible representations – might help move beyond abstract or stereotypical notions of cyber risk and instead grasp the mechanics of threats more concretely. This suggests that more tangible forms of comprehension may enable micro-businesses to make more accurate risk assessments, as seeing potential attacks brings both their likelihood and their consequences into sharper focus.

Table 11. User-need incongruences by code and sub-code, with proportional representation and pairwise agreement.

Need code category (Number of needs)	Proportion of incongruent sub code needs	Incongruent needs	Pairwise congruence
Guidance (17)	18%	Bring threats to life	DD & DB ✓ DE & DD ✗ DE & DB ✓
		Reach me	DD & DB ✗ DE & DD ✗ DE & DB ✓
		Right amount to spend	DD & DB ✓ DE & DD ✗ DE & DB ✓
Posture (10)	10%	Governance	DD & DB ✓ DE & DD ✗ DE & DB ✗
Resources (4)	0%	None	N/A
ROI (5)	60%	Reputation	DD & DB ✗ DE & DD ✓ DE & DB ✗
		Safer	DD & DB ✗ DE & DD ✓ DE & DB ✓
		Winning business	DD & DB ✓ DE & DD ✗ DE & DB ✗

Table 12. Guidance-related user needs compared with SME cybersecurity literature.

Finding	Sub code need
Confirms	Actionable: Khan et al. (2025a) concluded SMEs need guidance framed as actionable steps rather than abstract principles.
Confirms	Bite Sized: Wilson et al. (2023) found participants wanted short, digestible pieces of training and guidance.
Extends	Bring Threats To Life: Hoppe, Gatzert, and Gruner (2021), found that SMEs often lacked a clear understanding of threats. Our study extends this by showing that micro-businesses specifically need to *see threats visually* to better comprehend their nature and risks.
Confirms	Comparisons: Haney and Lutters (2018), through interviews with SME cyber consultants, found that SMEs often struggled to interpret and evaluate different cybersecurity products.
Confirms	Engaging: Khan et al. (2025) observed that much available SME cybersecurity guidance was text-heavy and failed to hold users' attention
Confirms	Finding Help: Renaud and Ophoff (2021) found that SMEs needed to be able to actually find / locate cybersecurity expertise
Confirms	List: Renaud and Weir (2016), found SMEs preferred check lists of things to do over abstract guidance
Confirms	Longevity: Haney and Lutters (2018) found SMEs need ongoing help rather than one time only support.
Confirms	No FUD*: Bada and Nurse (2019) found that fear appeals in cybersecurity engagement risks disengaging SMEs rather than motivating them.
Confirms	No Hard Sell: Haney and Lutters (2018) found SMEs were frustrated by sales-driven vendor approaches.
Confirms	Reach Me: Renaud and Ophoff (2021) observed that SMEs prefer guidance to reach them automatically, rather than requiring them to actively search for it.
Extends	Right Amount To Spend: While previous studies highlight limited finances as a barrier for SMEs (e.g. Cartwright and Cartwright 2025), our findings reveal a related but distinct need: micro-businesses want clarity on how much they should invest. Although the right figure will vary by size, sector, and risk profile, the demand for clear guidance on appropriate spending was evident.
Confirms	Scale Up Actions: Hoppe, Gatzert, and Gruner (2021) found that SMEs often fail to revisit cybersecurity measures as they expand, leaving emerging risks unmanaged.
Confirms	Simple: The literature consistently highlights SMEs' need for simple, jargon-free, non-technical security guidance they can easily understand (e.g. Renaud and Weir 2016).
Confirms	Tailored: The literature consistently stresses that SMEs require tailored, context-specific support aligned to their size, sector, and circumstances (e.g. Shojaifar and Järvinen 2021).
Confirms	Trust Source: A consistent finding across the literature is that SMEs want support from sources they trust. (e.g. Renaud and Ophoff (2021)).
Confirms	Understanding What to Prioritise: Ncubukezi, Mwansa, and Rocaries (2020) found that SMEs often struggle to identify which security actions to prioritise from the many available.

* FUD = Fear, Uncertainty and Doubt (Fear appeals).

Similarly, while limited financial resources are frequently cited as a barrier to cybersecurity adoption (e.g. Button et al. 2026), the identified need to understand how much to spend reveals a more nuanced challenge. For some micro-businesses, the issue appears less about unwillingness or absolute lack of funds and more about uncertainty regarding what they should be spending. This tension is particularly salient given persistent concerns in the SME literature about overcharging or being misled by private-sector providers (Cartwright, Cartwright, and Edun 2023), and concerns that many SMEs underinvest in cybersecurity and consequently leave themselves vulnerable (Cartwright and Cartwright 2025). In the absence of clear financial benchmarks or reference points, micro-business owners may struggle to judge what constitutes sufficient or appropriate expenditure. Supporting calibration of cybersecurity spending may therefore be as important as reducing costs themselves.

Taken together, the prominence and pattern of Guidance-related needs point to a structural gap in how cybersecurity support is currently framed and delivered to micro-businesses. Rather than lacking information per se, owners appear to lack mechanisms for prioritising actions, interpreting relevance, calibrating investment, and integrating cybersecurity practices into their everyday workflows. This suggests that effective intervention design may depend less on increasing the volume of guidance available and more on restructuring how guidance is sequenced, framed, and delivered so that it aligns with the operational realities and constraints of micro-business decision-makers.

4.1.2. Cybersecurity posture needs

4.1.3. Cybersecurity resource needs

4.1.4. Cybersecurity return on investment (ROI) needs

ROI has long been recognised as a problem area in SME cybersecurity. Prior studies show that SMEs often view cybersecurity as a cost with little visible payback, particularly when benefits are framed in preventive rather

Table 13. Posture-related user needs compared with SME cybersecurity literature.

Findings	Sub code need
Confirms	Assessing IT Suppliers Competence: Cartwright, Cartwright, and Edun (2023) found that SMEs often assume their IT suppliers are competent but rarely verify this.
Confirms	Boundaries: Chidukwani, Zander, and Koutsakis (2026) found that SMEs often lack clarity about where their responsibilities end and a provider's begin
Confirms	Doesn't Hinder: Cartwright, Cartwright, and Edun (2023) reported that some SMEs felt security often imposed restrictions or lengthy procedures that slowed productivity.
Confirms	Governance: Van Haastrecht et al. (2021) found that SMEs often lack awareness of cybersecurity regulations and struggle to understand their legal obligations (e.g. GDPR).
Confirms	Hackers: Bitzer, Stahl, and Strobel (2021) found that SMEs often have only a superficial understanding of cybercriminals, tending to see them as distant actors or irrelevant to their own context.
Confirms	Identifying My Threats: Rawindaran et al. (2023) found that SMEs often struggled to identify the cyber threats relevant to their business.
Confirms	Identifying My Weaknesses: Saban, Rau, and Wood (2021) found that SMEs often lack the ability to assess where their systems are vulnerable, noting that they rarely conduct structured vulnerability or risk assessments.
Confirms	Monitoring: Prior work notes that SMEs rarely have monitoring capabilities, such as Security Operations Centres (SOCs) (Chidukwani, Zander, and Koutsakis 2022) or Managed Detection and Response (MDR) services (Wilson et al. 2023).
Confirms	News Relevancy: Prior work links cyber-attack news to fear appeals (Bada and Nurse 2019) and SMEs struggling to judge whether such reports are relevant to their own business context (Wilson et al. 2023).
Confirms	Quantifying Risk: Hoppe, Gatzert, and Gruner (2021) found SMEs rarely quantify cyber risks, relying instead on intuition or qualitative judgments.

Table 14. Resource-related user needs compared with SME cybersecurity literature.

Findings	Sub code need
Confirms	Allocating Resource: Cartwright, Cartwright, and Edun (2023) found SMEs often deprioritized security, against other competing business demands.
Confirms	Expertise: Alahmari and Duncan (2020) found that most SMEs lacked dedicated security staff, with responsibility often falling to someone with a general IT interest.
Confirms	Money: Lack of funding for cybersecurity is a common theme in the literature (e.g. Renaud and Weir 2016).
Confirms	Time: Lack of time to engage with cybersecurity is a recurring finding in the literature (e.g. Alahmari and Duncan 2021).

than revenue-generating terms (Kosutic and Pigni 2022). This framing makes it difficult for owners to justify expenditure compared with other business investments that promise clearer growth or productivity gains (Hoppe, Gatzert, and Gruner 2021). Our findings extend this literature by identifying a different but related need – once micro-businesses have invested in cybersecurity, they want to be able to determine whether that investment is actually paying dividends. The issue here is not simply that ROI is viewed as a cost-versus-value judgement, but rather that businesses lack ways of evaluating whether their investment is working.

Table 15. ROI-related user needs compared with SME cybersecurity literature.

Findings	Sub code need
Confirms	Alleviate Worry: Hoppe, Gatzert, and Gruner (2021) noted that once SMEs engaged in awareness-raising exercises (like demos or visualisations) and adopted recommended mitigations, they reported greater confidence and reduced fear of attack.
Extends	Determining ROI: Research on SME cybersecurity ROI is limited. Prior work notes that SMEs often see little or no return (Wilson et al. 2023) or fail to link risk management with financial outcomes (Hoppe, Gatzert, and Gruner 2021). Our study advances this by identifying an explicit need for micro-businesses to determine whether their cybersecurity spend delivers value.
Confirms	Reputation: Barlette, Gundolf, and Jaouen (2017), in their SME CEO survey, found that protecting business reputation was a key driver of cybersecurity investment, particularly to avoid the negative PR fallout of an attack. SMEs feared losing clients and business opportunities if their reputation was damaged.
Confirms	Safer: Wilson et al. (2023) found that SMEs often fail to connect security actions with outcomes, leaving them uncertain whether measures truly reduce risk.
Confirms	Winning Business: Kosutic and Pigni (2022) emphasise that cybersecurity should not only be seen as a cost but as a potential source of competitive advantage.

Specifically, owners need to know – is their investment genuinely protecting the business from attack, is it safeguarding reputation and preventing financial loss, and is it providing a competitive advantage by helping to win or retain customers? The implication is that micros' concern is not just about *whether* to spend on cybersecurity, but about *how to measure and quantify the impact of that spend once it has been made*. In theoretical terms, these concerns align with perceived benefits in HBM and coping appraisal trade-offs in PMT: micro-business owners appear to weigh whether protective actions are worthwhile given limited resources and competing priorities, and they evaluate benefits in business terms (trust, reputation, customer requirements, and opportunity) as well as harm avoidance (Barlette, Gundolf, and Jaouen 2017; Jamil et al. 2025).

This concludes our discussion of RQ1. The next section addresses RQ2, examining how cybersecurity needs differ across the Digitally Dependent and Digitally Based micro-business groups, while incorporating Digital Enabler inputs included as provider perspectives for contextualisation and triangulation.

4.2. RQ2. How do articulated user needs differ across micro-business subgroups (Digitally dependent and digitally based), and how do digital enabler perspectives contextualise and interpret these differences?

4.2.1. Guidance needs: group-level incongruences

Three key incongruences emerged within the Guidance category. First, Digital Enablers ($n = 6$), drawing on

their consultancy experience supporting SMEs, highlighted more frequently the need to *bring threats to life* than Digitally Dependent participants ($n = 2$), while Digitally Based firms ($n = 3$) showed a similar pattern. This divergence between micro-business reports and Digital Enabler perspectives suggests a potential awareness gap: while Digitally Based participants and Digital Enabler perspectives indicate an appreciation of the value of making threats tangible, Digitally Dependent participants may lack the IT knowledge or experience to perceive and articulate this need. This finding aligns with Shojaifar and Järvinen (2021), who note that different SME groups often fail to recognise certain cybersecurity needs because these are not framed in ways that resonate with their context. They argue that providers must tailor and contextualise cybersecurity concepts within SMEs' operational realities to make such needs more visible and actionable, suggesting that solutions aimed at *bringing threats to life* could themselves help achieve this contextualisation.

While all groups expressed difficulty in *finding help*, the need for guidance to *reach businesses automatically* was voiced most by Digitally Dependents ($n = 6$), compared with Digitally Based ($n = 1$) and Digital Enabler perspectives ($n = 2$). This reflects a difference not in 'if' help is needed, but in 'how' it is obtained. Dependents appear to prefer push-based delivery, likely due to time pressures and our sample's younger business age, suggesting they are in start-up or growth phases with less capacity to seek support. In contrast, Based firms, being slightly older and digitally literate, appear more comfortable finding guidance proactively. However, their continued difficulty locating support suggests that the challenge is one of visibility and accessibility rather than motivation. Notably, this need was less evident in Digital Enabler perspectives, which may indicate a mismatch between how support is provided and how micro-businesses seek and access guidance. This pattern echoes earlier studies showing that SMEs frequently struggle to identify and access trustworthy cybersecurity assistance with engagement occurring reactively, prompted by events or external cues (Renaud and Ophoff 2021).

Questions about *how much to spend* on cybersecurity were raised most often by Digital Enablers ($n = 5$), compared with Digitally Based ($n = 2$) and Digitally Dependent ($n = 1$) participants. Enabler perspectives focused less on SMEs' ability to afford cybersecurity and more on how spend available budget wisely. This supports prior findings that SMEs often deploy their budgets reactively or inefficiently, investing without a clear understanding of risk exposure or return on investment (Hoppe, Gatzert, and Gruner 2021). For Enablers, the issue is strategic, allocating resources for maximum value, whereas for the other groups, uncertainty persists over what constitutes adequate investment. Improving financial literacy around cybersecurity spending could therefore help all groups move from questioning *why* to invest toward understanding *how* to invest wisely.

4.2.2. Posture needs: group-level incongruences

Support for *governance* and *regulatory compliance* was identified predominantly in Digital Enabler perspectives ($n = 7$), reflecting providers' observations of regulatory challenges faced by SMEs, compared with limited mentions from Digitally Based ($n = 2$) and none from Digitally Dependent participants ($n = 0$). This pattern suggests a gap between issues recognised by providers working across multiple SMEs and those articulated by micro-business participants, indicating that Dependent and Based groups may have more limited awareness of relevant regulatory requirements. Van Haastrecht et al. (2021) describe this as an 'institutional visibility gradient', where awareness of compliance obligations increases with digital maturity and ecosystem exposure. It may be that our Dependent and Based participants are yet to encounter such compliance demands.

4.2.3. ROI needs: group-level incongruences

Compared to Guidance (18%), Posture (10%), and Resources (0%), ROI-related needs showed the highest proportion of incongruence (60%). This indicates that perceptions of 'cybersecurity value' vary more strongly with a micro's IT context than its Guidance, Posture, or Resource considerations.

Reputation was raised most frequently by Digitally Based firms ($n = 9$), compared with Digitally Dependent ($n = 1$) and Digital Enabler perspectives ($n = 4$). For Based firms, whose credibility relies heavily on digital trust and service reliability, the need to protect reputation appears to be a critical concern. This aligns with prior research showing that SMEs in digitally focused sectors view cybersecurity as central to maintaining trust and client relationships (Wolf, Aviv, and Kuber 2021). For Dependents, whose operations are less digitally service-oriented, reputational harm may be perceived as a secondary issue. The moderate emphasis within Digital Enabler *reputation* perspectives suggests a more strategic, provider-informed orientation, where reputation is embedded within broader notions of value creation and competitive positioning. This interpretation is supported by the *Winning Business* need, where five Enablers – compared with one Dependent and one Based – explicitly give perspectives that linked cybersecurity to long-term growth and

market differentiation. This reflects the paradigm shift identified by Kosutic and Pigni (2022), whereby solutions are needed to help businesses move beyond viewing cybersecurity solely as a protective cost and instead recognise it as a potential source of strategic and competitive advantage.

4.2.4. Cross-category synthesis of incongruent needs

In summary, while resource constraints appear universal, some needs related to Guidance, Posture, and ROI vary according to ICT context. From a solutions perspective, this provides further evidence that 'one size fits all' interventions are unlikely to be effective. Instead, cybersecurity support across these categories may be more appropriately structured through tiered approaches aligned with levels of digital maturity. Importantly, the value of articulating and comparing these needs across subgroups lies not simply in identifying differences, but in understanding how those differences shape the interventions likely to be effective – an approach consistent with human-centered design, which emphasises defining requirements in ways that enable comparison across stakeholder groups and surface tensions in what different users require from a system or service (ISO 2019; Radnejad, Sarkar, and Osiyevskyy 2022). By identifying where Digitally Dependent and Digitally Based participants converge and diverge, and interpreting these patterns alongside Digital Enabler perspectives, the present analysis moves beyond treating SMEs as a homogeneous group and instead reveals the underlying differences and tensions that effective interventions must address.

The next section draws on the literature to identify potential interventions and examines them further in relation to RQ3.

4.3. RQ3. What literature-informed approaches could address the identified user needs?

Tables 16–19 map literature-informed approaches to the identified Guidance, Posture, Resource, and ROI needs. Where needs diverged between Digitally Dependent and Digitally Based participants, and/or diverge from Digital Enabler perspectives, approaches are noted as being more relevant to specific groups. Where all groups aligned, approaches are deemed universally relevant.

Having considered the research questions, the discussion now turns to the study's approach, its limitations, and directions for future research.

4.4. Reflections upon approach

Reflecting on the usefulness of a user-needs-led approach for improving understanding of the micro-business cybersecurity problem space, the findings suggest that it yielded relatively limited new insights into barriers to cybersecurity adoption. A small number of identified needs marginally extend existing knowledge by surfacing under-articulated nuances that may warrant greater attention in the design of cybersecurity interventions. However, generating new findings was not the primary rationale using this approach. Rather, the intention was translational: to synthesise insights from micro-business interviews into a structured set of cybersecurity user needs and then draw on the extant literature to identify ways of addressing those needs. A key point for reflection, therefore, is to consider how successful this synthesis has been and whether it has produced a set of needs that are both practical to use and genuinely valuable for informing cybersecurity service design.

Empirically assessing whether the needs achieve these outcomes falls beyond the scope of the present study. However, based on our anecdotal observations, the user needs presented in this study appear straightforward to apply: they require little training to interpret, can be quickly reviewed, and readily support ideation through 'How might we … ?' questions. Ultimately, however, the real-world impact of this approach will depend on how the needs are applied in service design practice. As highlighted in ISO 9241-210, the value of user-centered design (UCD) outputs is greatest when they are incorporated into genuinely iterative design and evaluation processes, rather than treated as a static checklist.

Reflecting on the coverage of the identified needs, the extant UCD literature recognises that user needs are not always readily articulated, may evolve over time, and can be shaped by elicitation methods and contextual factors (Rooney and Jelenewicz 2026). Accordingly, the needs presented in this study should not be interpreted as definitive or exhaustive, but rather as a first step in applying a UCD perspective to the micro-business cybersecurity domain. At the same time, there are indications that our findings are credible. First, the identified needs align closely with themes repeatedly documented in the SME cybersecurity literature. Second, qualitative research guidelines suggest that thematic saturation is often reached within approximately 9–17 interviews (Hennink and Kaiser 2022). Therefore, the 30 interviews conducted in this study may provide additional confidence that most needs were identified, even if not exhaustively.

Table 16. Literature-informed approaches for addressing micro cybersecurity guidance needs.

User need	Literature informed approaches
Actionable	Frame guidance as concrete, actionable steps rather than abstract principles (Khan et al. 2025a).
Bite Sized	Prerecorded, point-of-need modules that could be replayed for easier access (Wilson et al. 2023).
Bring Threats to Life	This need was more pronounced among Dependents, who were incongruent with Enabler perspectives. Hacking demonstrations and case studies may help make cyber threats more tangible and improve understanding of the risks they pose (Osborn and Simpson 2018).
Comparisons	Independent reviews or regulator-endorsed benchmarks of cybersecurity products (Haney and Lutters 2018).
Engaging	Use engaging formats, such as visualisations, videos, and interactive resources (Khan et al. 2025a)
Finding Help	Increase awareness of available support channels and how to engage with them (Renaud and Ophoff 2021).
List	Provide checklists (Renaud and Dupuis 2016).
Longevity	Prioritise long-term advisory support over single, transactional engagements (Haney and Lutters 2018).
No Fear Appeals	Replace fear based content with supportive and constructive messaging (Bada and Nurse 2019), except when addressing misconceptions e.g. *I'm too small to be attacked*. In such cases, targeted fear appeals may be appropriate, provided that they are accompanied by clear guidance on how to reduce the identified risks (Renaud and Dupuis 2019).
No Hard Sell	Avoid sales-driven or 'hard sell' approaches (Haney and Lutters 2018).
Reach Me	This need was more pronounced among Dependents. Deliver cybersecurity advice through existing SME channels, such as chambers of commerce (Renaud and Ophoff 2021).
Right Amount To Spend	This need was more pronounced among Dependents, who were incongruent with Enabler perspectives. Clearer spending guidance is required; however, prescriptive benchmarks risk being misleading/ anti-competitive given that optimal cybersecurity investment is inherently uncertain and highly business-specific, making it difficult for businesses to judge appropriate expenditure (Rawindaran et al. 2023). While indicative ranges (e.g. £10 - £50 per employee; Osborn and Simpson 2018) may provide a useful starting point, adaptive tools, such as risk-based calculators or sector-specific benchmarks, are likely to better support decision-making.
Scale Up Actions	Embed threat reassessment and the scaling of cybersecurity controls within regular business growth cycle (Hoppe, Gatzert, and Gruner 2021)
Simple	Provide simple, jargon-free cybersecurity guidance that micro-businesses can easily understand (e.g. Renaud and Weir 2016).
Tailored	Provide tailored, context-specific cybersecurity support aligned to business size, sector, and circumstances rather than generic 'one size fits all' approaches (e.g. Shojaifar and Järvinen 2021).
Trust Source	Help SMEs recognise trustworthy support channels (e.g. government, regulators, police) (Renaud and Ophoff 2021).
What to Prioritise	Develop context-aware risk assessment frameworks that rank or filter actions by SME size and age (Cartwright and Cartwright 2025).

It is important to acknowledge that adopting a user-needs-led approach on its own will not resolve all the challenges associated with making cybersecurity

Table 17. Literature-informed approaches for addressing micro cybersecurity posture needs.

User need	Literature informed approaches
Assessing IT Suppliers Competence	SMEs should seek accreditations, certifications, or third-party assurance schemes to verify supplier competence (Cartwright, Cartwright, and Edun 2023)
Boundaries	Increase transparency and education to help SMEs understand where their responsibilities end and a providers begin (Haney and Lutters 2018).
Doesn't Hinder	Automate tasks such as patch management outside business hours so protections are maintained without disrupting operations (Van Haastrecht et al. 2021).
Governance	Enablers perspectives were incongruent with the other groups, suggesting that Digitally Dependent and Digitally Based participants may benefit from greater regulatory awareness to strengthen their understanding of cybersecurity obligations (Van Haastrecht et al. 2021).
Hackers	Include attacker profiles, motives, and methods in awareness efforts so micros better understand why they may be targeted (Bitzer, Stahl, and Strobel 2021).
Identifying My Threats	Provide regular threat briefings and tailored intelligence linked to relevant mitigations (Hoppe, Gatzert, and Gruner 2021).
Identifying Weaknesses	Encourage SMEs to conduct gap analyses or structured vulnerability assessments to proactively identify weaknesses (Chidukwani, Zander, and Koutsakis 2022).
Monitoring	Improve awareness of monitoring options such as Security Operations Centers (SOC), Security Information and Event Management (SIEM) or Detection and Response (MDR) services to raise awareness of available solutions (Van Haastrecht et al. 2021).
News Relevancy	Provide sector-specific digests that filter cyber-attack news by industry, size, and relevance, paired with contextualised guidance to help organisations interpret potential implications (e.g. 'This attack on a logistics firm matters if you use supplier X - here's what to check') (Wolf, Aviv, and Kuber 2021).
Quantifying Risk	Provide simplified frameworks (e.g. likelihood × impact matrices) that map security actions to measurable risk reduction (e.g. 'spam filters block X% of phishing emails') (Hoppe, Gatzert, and Gruner 2021).

Table 18. Literature-informed approaches for addressing micro cybersecurity resource needs.

User need	Literature informed approaches
Allocating Resource	Raise awareness of the risks of postponing cybersecurity and promote phased approaches (e.g. implement basic hygiene first, advanced measures later), embedding security into everyday business processes (Cartwright and Cartwright 2025).
Expertise	Increase access to cybersecurity expertise by raising awareness of available UK Government support and promoting affordable shared-service options, such as virtual CISOs (Wilson et al. 2023).
Money	Promote financial accessibility by signposting free or subsidised government support and encouraging providers to offer low-cost, flexible payment options (Renaud and Ophoff 2021).
Time	Save time by promoting automated updates, managed services, and awareness of the risks created when security tasks are delayed due to time pressures (Wilson et al. 2023).

Table 19. Literature-informed approaches for addressing micro cybersecurity ROI needs.

User need	Literature informed approaches
Alleviate Worry	Show businesses the tangible impact of their protective actions through follow-ups, feedback, or progress dashboards so they can see their efforts paying off (Khan et al. 2025a).
Determining ROI	Develop specific ROI frameworks with KPIs such as reduced downtime, improved customer trust, or avoided costs. Mechanisms could include tender success tracking, customer satisfaction surveys, or cost-avoidance metrics that connect cybersecurity actions with measurable business performance (Kosutic and Pigni 2022).
Reputation	Digitally Based firms were incongruent Dependents and Enabler perspectives in this need. Solutions may involve obtaining trusted certifications and promoting compliance through customer-facing materials (e.g. websites, proposals) to signal trust and reliability to clients and partners (Barlette, Gundolf, and Jaouen 2017).
Safer	Based businesses were incongruent with Dependents in this need, indicating a desire for reassurance that security measures are effective. Solutions could include demonstrating the impact of protections (e.g. showing that a spam filter blocked specific phishing attempts) to reinforce confidence that investments reduce risk (Wilson et al. 2023).
Winning Business	Enabler perspectives were incongruent with the other groups expressions of this need, suggesting that Dependents and Based firms may need solutions that help them recognise cybersecurity as a strategic differentiator. Such solutions could demonstrate how security investments create competitive advantage, for instance, by meeting procurement standards, strengthening customer trust, or improving supplier relationships (Kosutic and Pigni 2022).

guidance for SMEs more understandable and actionable. Nor does the articulation of user needs overcome the persistent difficulties of bridging academic insights into industry practice, or of encouraging non-academic audiences to engage with and apply them. Furthermore, in organisations where cybersecurity decisions involve multiple stakeholders, needs may vary between individuals. Such variation introduces additional complexity in determining which needs should be prioritised and what types of solutions may be appropriate in such scenarios.

Finally, reflecting on the use of the Health Belief Model (HBM) to inform the interview design, the the theoretical grounding of the questions appears methodologically appropriate, given that reviews suggest that studies drawing on established behavioural theory are more effective at eliciting meaningful behavioural insights than those relying on atheoretical or ad hoc questioning approaches (Dalgetty, Miller, and Dombrowski 2019). However, selecting HBM rather than Protection Motivation Theory (PMT) may have constrained exploration of how threat appraisal and coping appraisal interact to shape protective motivation, particularly in the context of threat or fear-based cybersecurity messaging. Consequently, the study may have missed some explanatory nuance related to threat appraisal, which could have influenced both the identification and interpretation of threat (Posture)-related needs and the Guidance need concerning the avoidance of fear, uncertainty, and doubt messaging.

Having reflected on the approach used in this study, we now turn to the broader limitations and contextual constraints that shape its findings.

4.5. Limitations

This study has several methodological limitations. While most interviewees were micro-businesses, two participants within the Digitally Based group were small firms (10–49 employees) at the lower end of that range. Although recruiting ten Digitally Based micro-businesses would have been preferable, only eight were secured, reflecting the well-documented challenges of recruiting SMEs for cybersecurity research (Osborn and Simpson 2018). Their inclusion is unlikely to have materially affected the findings, as their responses closely aligned with those of the micro-business participants and did not introduce substantively different patterns.

Interviews were relatively short (approximately 20 min), which was a deliberate strategy to encourage participation from micro-business owners who are often highly time-constrained and sensitive to participation demands (Wilson et al. 2023). While the shorter duration may have limited the depth of some responses and the identification of certain needs, this represents a pragmatic trade-off commonly encountered when engaging SME participants. For example, Alahmari and Duncan (2021) report distributing interview invitations to hundreds of participants, yet only 20 agreed to participate. In the present study, 30 interviews were conducted, generating approximately 10 h of qualitative data. When considered alongside the strong alignment between the identified needs and the existing SME cybersecurity literature, this provides reasonable assurance that the study captured meaningful and substantively relevant insights despite the relatively short interview duration.

The congruence analysis across the Digitally Dependent, Digitally Based groups and Digital Enabler perspectives used a ≥ 4 interviewee threshold to identify meaningful differences. While this threshold is inherently somewhat arbitrary, it was selected as a pragmatic balance: lower thresholds risk overstating apparent congruence between groups, while higher thresholds risk obscuring meaningful variation in responses.

The sample in this study is relatively small and not statistically representative, with most participants affiliated with UK Cyber Resilience Centers (CRCs).

However, the sample size is comparable to other interview-based studies in SME cybersecurity research, where recruitment often relies on snowball or network-based sampling approaches (e.g. Khan et al. 2025a). Such strategies are frequently adopted due to the well documented difficulty of recruiting SMEs through conventional sampling methods; for example, Osborn and Simpson (2018) report that attempts to recruit SMEs through random sampling of mailing lists produced response rates of less than 1%. While this approach enabled the recruitment of participants who might otherwise have been difficult to engage, it may have introduced a degree of positive bias. Businesses connected to CRC networks may possess higher levels of cybersecurity awareness and greater access to support than those outside such networks, which may have influenced the salience or absence of certain identified needs.

Finally, the predominance of UK-based participants limits the contextual generalizability of the findings. Organisations operating in other jurisdictions may face different regulatory, institutional, and cultural conditions that shape their cybersecurity needs, particularly in relation to non-UK regulatory frameworks.

4.6. Directions for future research

An important avenue for future research is to evaluate whether the identified needs can meaningfully improve cybersecurity service design and engagement. Empirical studies involving SME cybersecurity practitioners could examine whether applying these needs in practice leads to more effective and user-aligned service design. Extending the user-needs synthesis to small and medium-sized firms would also enable comparative analyses across SME subgroups and support the development of more targeted cybersecurity interventions.

4.7. Conclusion

This study set out to adopt a user-needs-led, UCD-informed approach to understanding micro-business cybersecurity and to translate qualitative insights into a structured, design-relevant benchmark of user needs. The primary contribution lies not in identifying entirely novel barriers, but in synthesising existing cybersecurity insights and articulating them in the voice of micro-business decision makers. By organising 36 user needs across the categories of Guidance, Posture, Resources, and ROI, the study provides a translational framework that others can use to improve cybersecurity service design. The findings indicate that micro-business cybersecurity engagement is driven less by threat awareness alone and more by the need for actionable, simple, and contextually tailored guidance that reduces cognitive load and fits within the severe time, resource, and expertise constraints faced by micro-business owners. Subgroup analysis further demonstrates that cybersecurity needs are not homogeneous across Digitally Dependent and Digitally Based contexts, nor do they align consistently with Digital Enabler perspectives, reinforcing the limitations of 'one-size-fits-all' engagement strategies. Importantly, the identified literature-informed solutions are design considerations rather than validated interventions, offered to illustrate how a user-needs-led framing can support more targeted and contextually grounded cybersecurity guidance. Accordingly, this research should be viewed as an initial step toward opening an 'opportunity space' for designing more user-aligned cybersecurity interventions. More broadly, it reframes micro-business cybersecurity not solely as a technical capability gap or a matter of owner behaviour, but as a translational design challenge in which the effectiveness of support depends on how clearly cybersecurity insights are communicated, structured, and aligned with the realities of micro-business contexts.

Acknowledgements

We would like to thank all interviewees who generously gave their time to participate in this study, as well as the CRC network for facilitating participant recruitment through their membership base. We also thank the reviewers for their constructive feedback and the time they devoted to the review process.

Author contributions

CRediT: **Martin Wilson:** Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Project administration, Resources, Visualization, Writing – original draft, Writing – review & editing; **Sharon Mcdonald:** Conceptualization, Supervision, Writing – original draft; **Alastair Irons:** Supervision, Writing – review & editing; **Joe Cockcroft:** Formal analysis.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Data availability statement

The participants of this study did not give written consent for their data to be shared publicly, so due to the sensitive nature of the research, supporting data is not available.

ORCID

Martin Wilson http://orcid.org/0000-0001-8886-6527
Sharon Mcdonald http://orcid.org/0000-0002-4774-634X
Alastair Irons http://orcid.org/0000-0002-5174-6596
Joe Cockcroft http://orcid.org/0009-0001-0183-3739

References

Alahmari, A., and B. Duncan. 2020. Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA),* Dublin, Ireland, 15–19 June 2020, 1–5. IEEE. https://doi.org/10.1109/CyberSA49311.2020.9139638

Alahmari, A. A., and R. A. Duncan. 2021. Investigating potential barriers to cybersecurity risk management investment in SMEs. In 2021 *13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)* (pp. 1–6). IEEE. https://doi.org/10.1109/ECAI52376.2021.9515166

Aranitou, V., and C. Arachovas. 2024. "SMES and Large Enterprises: A Preliminary Comparative Analysis." In *The Economic Impact of Small and Medium-Sized Enterprises: Analytical Approaches to Growth and Innovation Challenges amid Crises in Europe*, edited by V. Aranitou, M. Manioudis, and A. Angelakis, 41–52. Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-74554-6_3

Bada, M., and J. R. Nurse. 2019. "Developing Cybersecurity Education and Awareness Programmes for Small- and Medium-Sized Enterprises (SMEs)." *Information & Computer Security* 27 (3): 393–410. https://doi.org/10.1108/ICS-07-2018-0080.

Barlette, Y., K. Gundolf, and A. Jaouen. 2017. "CEOs' Information Security Behavior in SMEs: Does Ownership Matter?" *Systèmes D'information & Management* Volume 22 (3): 7–45. https://doi.org/10.3917/sim.173.0007.

Bernard, H. R. 2017. *Research Methods in Anthropology: Qualitative and Quantitative Approaches* (6th ed.). Lanham, MD: Rowman & Littlefield.

Bitzer, M., B. Stahl, and J. Strobel. 2021. Empathy for Hackers—An IT Security Risk Assessment Artifact for Targeted Hacker Attacks. In *Proceedings of the 29th European Conference on Information Systems (ECIS)* (pp. 1–15). Association for Information Systems. https://aisel.aisnet.org/ecis2021_rp/170.

Braun, V., and V. Clarke. 2013. *Successful Qualitative Research: A Practical Guide for Beginners*. London: SAGE Publications.

Button, D. J., J. Ophoff, A. Irons, and S. McDonald. 2026. "Mind the Gap: Exploring Perceptions of Cyber Security in the SME Context." *Information & Computer Security* 34 (2): 231–245. https://doi.org/10.1108/ICS-02-2025-0047.

Cartwright, A., and E. Cartwright. 2025. "Underinvestment in Cyber Security: Quantifying Cyber Security Behavior in UK Businesses." *Journal of Small Business Management*: 1–36. https://doi.org/10.1080/00472778.2025.2549068.

Cartwright, A., E. Cartwright, and E. Edun. 2023. "Cascading Information on Best Practice: Cyber Security Risk Management in UK Micro and Small Businesses and the Role of IT Companies." *Computers & Security* 131:103288. https://doi.org/10.1016/j.cose.2023.103288.

Chidukwani, A., S. Zander, and P. Koutsakis. 2022. "A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations." *IEEE Access* 10:85701–85719. https://doi.org/10.1109/ACCESS.2022.3197899.

Chidukwani, A., S. Zander, and P. Koutsakis. 2026. "Beyond Self-reporting: Uncovering the Operational Realities of SME Cybersecurity through Expert Assessment." *Computers & Security* 164:104839. https://doi.org/10.1016/j.cose.2026.104839.

Chute, C., T. French, S. Raman, and J. Bradley. 2022. "User Requirements for Comanaged Digital Health and Care: Review." *Journal of Medical Internet Research* 24 (6): e35337. https://doi.org/10.2196/35337.

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.

Dalgetty, R., C. B. Miller, and S. U. Dombrowski. 2019. "Examining the Theory-Effectiveness Hypothesis: A Systematic Review of Systematic Reviews." *British Journal of Health Psychology* 24 (2): 334–356. https://doi.org/10.1111/bjhp.12356.

Department for Business and Trade (DBT). 2024, October 3. *Business Population Estimates for the UK and Regions 2024: Statistical Release*. GOV.UK. https://www.gov.uk/government/statistics/business-population-estimates-2024/business-population-estimates-for-the-uk-and-regions-2024-statistical-release.

Department for Science, Innovation and Technology (DSIT). 2024, April 9. *Cyber Security Breaches Survey* 2024. GOV.UK. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024.

Department for Science, Innovation and Technology (DSIT). 2025a, February 10. *Government Digital Service*. GOV.UK. https://www.gov.uk/government/organisations/government-digital-service.

Department for Science, Innovation and Technology (DSIT). 2025b, June 19. *Cyber Security Breaches Survey* 2025. GOV.UK. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025.

Federation of Small Businesses. 2023. *UK Small Business Statistics: Business Population Estimates for the UK and Regions in* 2023. National Federation of Self Employed & Small Businesses Limited. https://www.fsb.org.uk/uk-small-business-statistics.html.

GOV.UK. 2017, March 23. *Users and Their needs - Service Manual*. https://www.gov.uk/service-manual/user-research/start-by-learning-user-needs.

Halpin, S. N. 2024. "Using Chat GPT to Clean Qualitative Interview Transcriptions: A Usability and Feasibility Analysis." *American Journal of Qualitative Research* 8 (3): 153–160. https://doi.org/10.29333/ajqr/14487.

Haney, J. M., and W. G. Lutters. 2018. "It's Scary … It's confusing … It's Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security. In *Proceedings of the 14th Symposium on Usable Privacy and Security (SOUPS)* (pp. 411–425). USENIX Association.

Heidt, M., J. P. Gerlach, and P. Buxmann. 2019. "Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments." *Information Systems Frontiers* 21 (6): 1285–1305. https://doi.org/10.1007/s10796-019-09959-1.

Hennink, M., and B. N. Kaiser. 2022. "Sample Sizes for Saturation in Qualitative Research: A Systematic Review of Empirical Tests." *Social Science & Medicine* 292:114523. https://doi.org/10.1016/j.socscimed.2021.114523.

Hoppe, F., N. Gatzert, and P. Gruner. 2021. "Cyber Risk Management in SMEs: Insights from Industry Surveys." *The Journal of Risk Finance* 22 (3/4): 240–260. https://doi.org/10.1108/JRF-02-2020-0024.

International Organization for Standardization (ISO). 2019. *ISO 9241-210:2019 Ergonomics of Human-System Interaction - Part 210: Human-Centred Design for Interactive Systems*. https://www.iso.org/standard/77520.html.

Jamil, H., T. Zia, T. Nayeem, M. T. Whitty, and S. D'Alessandro. 2025. "Human-centric Cyber Security: Applying Protection Motivation Theory to Analyse Micro Business Owners' Security Behaviours." *Information & Computer Security* 33 (1): 49–76. Advance online publication. https://doi.org/10.1108/ICS-10-2023-0176.

Junior, C. R., I. Becker, and S. Johnson. 2023. Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity (No. arXiv:2309.17186). *arXiv*. http://arxiv.org/abs/2309.17186.

Khan, N., S. Furnell, M. Bada, J. R. C. Nurse, and M. Rand. 2025a. "Assessing Cyber Security Support for Small and Medium-Sized Enterprises." In *Human Aspects of Information Security and Assurance: 18th IFIP WG 11.12 International Symposium, HAISA 2024, Skövde, Sweden, July 9–11, 2024, Proceedings, Part I*, edited by N. Clarke and S. Furnell, 148–162. Springer. https://doi.org/10.1007/978-3-031-72559-3_11

Khan, N., S. Furnell, M. Bada, J. R. C. Nurse, and M. Rand. 2026. "The Hidden Barriers to Cyber Security Adoption amongst Small and Medium-Sized Enterprises." *Information & Computer Security* 34 (4): 211–230. https://doi.org/10.1108/ICS-04-2025-0135.

Khan, N., S. Furnell, M. Bada, M. Rand, and J. R. C. Nurse. 2025b. "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.

Klein, V. B., and J. L. Todesco. 2020. "Constructing Customer Knowledge in Knowledge-Intensive Customer Relationships." *Knowledge and Process Management* 27 (2): 251–261. https://doi.org/10.1002/kpm.1650.

Kosutic, D., and F. Pigni. 2022. "Cybersecurity: Investing for Competitive Outcomes." *Journal of Business Strategy* 43 (1): 28–36. https://doi.org/10.1108/JBS-06-2020-0116.

Krippendorff, K. 2004. "Reliability in Content Analysis.." *Human Communication Research* 30 (3): 411–433. https://doi.org/10.1111/j.1468-2958.2004.tb00738.x.

Lo, O.-T., S.-P. Ng, S. Ng, V. Lai, and S. S. Y. Keung. 2025. "Unraveling the Nature of Design Thinking Disposition: Contributions of Trait Cognitive Flexibility and Trait Empathy on Design Thinking Potential." *Design Studies* 99:101325. https://doi.org/10.1016/j.destud.2025.101325.

Lowry, E., M. J. Hogan, J. Moriarty, O. M. Harney, E. Ruijer, M. Pilch, J. M. Groarke, M. Hanlon, and I. Shuttleworth. 2023. "Using Collective Intelligence Methods to Improve Government Data Infrastructures and Promote the use of Complex Data: The Example of the Northern Ireland Longitudinal Study." *Health Research Policy and Systems* 21:134. https://doi.org/10.1186/s12961-023-01070-x.

McGrath, C., P. J. Palmgren, and M. Liljedahl. 2019. "Twelve Tips for Conducting Qualitative Research Interviews." *Medical Teacher* 41 (9): 1002–1006. https://doi.org/10.1080/0142159X.2018.1497149.

Ncubukezi, T., L. Mwansa, and F. Rocaries. 2020. "A Review of the Current Cyber Hygiene in Small and Medium-Sized Businesses." *In 2020 15th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE*. https://doi.org/10.23919/ICITST51030.2020.9351339.

Ng, B.-Y., A. Kankanhalli, and Y. Xu. 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.

Osborn, E., and A. Simpson. 2018. "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.

Radnejad, A. B., S. Sarkar, and O. Osiyevskyy. 2022. "Design Thinking in Responding to Disruptive Innovation: A Case Study." *The International Journal of Entrepreneurship and Innovation* 23 (1): 39–54. https://doi.org/10.1177/14657503211033940.

Rae, A., and A. Patel. 2019. "Defining a new Composite Cybersecurity Rating Scheme for SMEs in the U.K." In *Information Security Practice and Experience (ISPEC 2019) (Lecture Notes in Computer Science)*. Vol. 11879, edited by S. H. Heng and J. Lopez, 291–306. Cham: Springer. https://doi.org/10.1007/978-3-030-34339-2_20.

Rawindaran, N., A. Jayal, E. Prakash, and C. Hewage. 2023. "Perspective of Small and Medium Enterprise (SME's) and Their Relationship with Government in Overcoming Cybersecurity Challenges and Barriers in Wales." *International Journal of Information Management Data Insights* 3 (2): 100191. https://doi.org/10.1016/j.jjimei.2023.100191.

Renaud, K., and M. Dupuis. 2019. "Should We Scare People into Behaving Securely?" *Network Security* 2019:20–20. https://doi.org/10.1016/S1353-4858(19)30135-7.

Renaud, K., and J. Ophoff. 2021. "A Cyber Situational Awareness Model to Predict the Implementation of Cyber Security Controls and Precautions by SMEs." *Organizational Cybersecurity Journal: Practice, Process and People* 1 (1): 24–46. https://doi.org/10.1108/OCJ-03-2021-0004.

Renaud, K., and G. R. S. Weir. 2016. Cybersecurity and the Unbearability of Uncertainty. In *Proceedings of the 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)* (pp. 137–143). IEEE. https://doi.org/10.1109/CCC.2016.29

Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change1." *The Journal of Psychology* 91 (1): 93–114. https://doi.org/10.1080/00223980.1975.9915803.

Rooney, S. I., and S. M. Jelenewicz. 2026. "Voice of the Customer Videos: An Educational Tool to Identify Unmet Clinical Needs and Develop Empathy for Medical Device Users." *Biomedical Engineering Education* 6 (1): 153–169. https://doi.org/10.1007/s43683-025-00206-5.

Rosenstock, I. M. 1974. "Historical Origins of the Health Belief Model." *Health Education Monographs* 2 (4): 328–335. https://doi.org/10.1177/109019817400200403.

Saban, K. A., S. Rau, and C. A. Wood. 2021. ""SME Executives' Perceptions and the Information Security Preparedness Model"." *Information & Computer Security* 29 (2): 263–282. https://doi.org/10.1108/ICS-01-2020-0014.

Saha, B., and Z. Anwar. 2024. "A Review of Cybersecurity Challenges in Small Business: The Imperative for a Future Governance Framework." *Journal of Information Security* 15 (1): 24–39. https://doi.org/10.4236/jis.2024.151003.

Schmieden, K. von. 2018, September 26. *Feeling in Control: Bank of America Helps Customers to "Keep the Change."* This Is Design Thinking! https://thisisdesignthinking.net/2018/09/feeling-in-control-bank-of-america-helps-customers-to-keep-the-change/.

Shojaifar, A., and H. Järvinen. 2021. Classifying SMEs for Approaching Cybersecurity Competence and Awareness. In *Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES 2021)* (pp. 1–7). ACM. https://doi.org/10.1145/3465481.3469200

Small Business Standards (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.

Such, J. M., P. Ciholas, A. Rashid, J. Vidler, and T. Seabrook. 2019. "Basic Cyber Hygiene: Does It Work?" *Computer* 52 (4): 21–31. https://doi.org/10.1109/MC.2018.2888766.

Suhaimi, Safia Najwa, Andrew Walters, and Jo. Ward. 2024. "Design Thinking Mindset: A User-Centred Approach toward Innovation in the Welsh Creative Industries." *International Journal of Design Creativity and Innovation* 12 (4): 238–257. https://doi.org/10.1080/21650349.2024.2383410.

Tam, T., A. Rao, and J. Hall. 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.

UK Government. 2006. *Companies Act* 2006. The National Archives. https://www.legislation.gov.uk/ukpga/2006/46/contents.

Van Haastrecht, M., B. Yigit Ozkan, M. Brinkhuis, and M. Spruit. 2021. "Respite for SMEs: A Systematic Review of Socio-Technical Cybersecurity Metrics." *Applied Sciences* 11 (15): 6909. https://doi.org/10.3390/app11156909.

Wilson, M., and S. McDonald. 2025. "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., S. McDonald, D. Button, and K. McGarry. 2023. "It Won't Happen to Me: Surveying SME Attitudes to Cyber-Security." *Journal of Computer Information Systems* 63 (2): 397–409. https://doi.org/10.1080/08874417.2022.2067791.

Wolf, F., A. J. Aviv, and R. Kuber. 2021. Security Obstacles and Motivations for Small Businesses from a CISO's Perspective. In: *Proceedings of the 30th USENIX Security Symposium (USENIX Security 21)*, August 2021, pp. 1199–1216. USENIX Association. https://www.usenix.org/conference/usenixsecurity21/presentation/wolf.

Zavattaro, F., and F. Gille. 2026. "The 30-Minute Interview Methods Guide: Lessons from over 100 Interviews in the Health Policy Domain." *International Journal of Qualitative Methods* 25: 1–8. https://doi.org/10.1177/16094069251414255.

Appendices

Appendix A

Table A1. Screening questions used to collect data from prospective digitally dependent and digitally based interviewees.

Question	Response options	Inspiration
What is your main sector?	Drop down list with 14 options	2025 Cyber Security Breaches Survey
Have you suffered a previous cyber-attack?	Yes/No Prefer not to say	Self-Developed
Which area of the UK is your business located in?	13 geographic locations including prefer not to say	2025 Cyber Security Breaches Survey
What is the size of your organization?	Micro (<10 employees) Small (11–50 employees) Medium (>51–250 employees)	UK Governments Companies Act 2006
Roughly, how many internet enabled devices does your business have? (e.g. laptops, desktops, mobile devices, servers etc.)	Enter number (free text)	Self-Developed
Do you have a standardised set of IT equipment which you procure for your business e.g. only Dell, HP or Apple?	Yes No	Self-Developed
Do you monitor logs? (logs are files which record network/computing events, which occur on your devices / systems)	Yes No Don't' Know	Self-Developed
What cybersecurity products / tools / assessments does your business use? (select all which apply)	Cyber essentials, ISO27001 Firewalls, Antivirus 2FA, IDS, Encryption Vuln assessments, Pen tests, Training, Backups, Other (please state)	Self-Developed
How dependent is your business on Information Technology?	HighlyS omewhatN ot at all dependent	Self-Developed
Does your company use an online bank account?	Yes No	Self-Developed
Does your company hold personal information about customers electronically? (e.g. names, dob, phone numbers, email addresses, postal addresses etc.)	Yes No	Self-Developed
Does your company allow customers to order, book or pay online.	Yes No	Self-Developed

Appendix B

Table A2. Codebook of themes and their applications in digitally dependent, digitally based and digital enabler interviews.

Code	Application
Cybersecurity Guidance	Interviewees' needs regarding the protective guidance they receive, including what they would like to see included, the support they require, and their expectations of cyber experts. For providers, this covers how SMEs have communicated these needs, or how providers perceive SMEs as having such needs.
Cybersecurity Posture	Interviewees' needs in assessing their current cybersecurity status from threat, protection, and risk perspectives – focusing on present activities and immediate requirements. For providers, this includes how SMEs articulate these needs, or how providers perceive SMEs as experiencing them.
Resources	Interviewees' needs related to resources (time, money, expertise), and how resource limitations contribute to the deprioritization of cybersecurity in favour of competing demands. For providers, this refers to how SMEs articulate these resource-related needs, or how providers perceive SMEs as experiencing such challenges.
Return on Investment (ROI)	Interviewees' needs concerning cybersecurity return on investment (ROI), including difficulties in measuring or demonstrating ROI. For providers, this covers how SMEs have expressed ROI-related needs, or how providers perceive SMEs as facing such challenges.