University of Kent

Kent Academic Repository

Khan, Neeshe, Furnell, Steven, Bada, Maria, Nurse, Jason R. C. and Rand, Matthew (2025) *The hidden barriers to cyber security adoption amongst Small and Medium-Sized Enterprises.* Information and Computer Security . ISSN 2056-4961.

Downloaded from
https://kar.kent.ac.uk/110491/ The University of Kent's Academic Repository KAR

The version of record is available from
https://doi.org/10.1108/ICS-04-2025-0135

This document version
Author's Accepted Manuscript

DOI for this version

Licence for this version
CC BY-NC (Attribution-NonCommercial)

Additional information
This author accepted manuscript is deposited under a Creative Commons Attribution Non-commercial 4.0 International (CC BY-NC) licence. This means that anyone may distribute, adapt, and build upon the work for non-commercial purposes, subject to full attribution. If you wish to use this manuscript for commercial purposes, please contact permissions@emerald.com.

Versions of research works

Versions of Record
If this version is the version of record, it is the same as the published version available on the publisher's web site. Cite as the published version.

Author Accepted Manuscripts
If this document is identified as the Author Accepted Manuscript it is the version after peer review but before type setting, copy editing or publisher branding. Cite as Surname, Initial. (Year) 'Title of article'. To be published in ***Title of Journal*** , Volume and issue numbers [peer-reviewed accepted version]. Available at: DOI or URL (Accessed: date).

Enquiries
If you have questions about this document contact ResearchSupport@kent.ac.uk. Please include the URL of the record in KAR. If you believe that your, or a third party's rights have been compromised through this document please see our Take Down policy (available from https://www.kent.ac.uk/guides/kar-the-kent-academic-repository#policies).

The hidden barriers to cyber security adoption amongst Small and Medium-Sized Enterprises

Neeshe Khan[1*], Steven Furnell[1], Maria Bada[2], Jason R.C. Nurse[3] , & Matthew Rand[2],

[1] School of Computer Science, University of Nottingham, Nottingham, UK
[2]Queen Mary University of London, London, UK
[3]University of Kent, Canterbury, UK

*Corresponding Author: neeshe.khan1@nottingham.ac.uk

Abstract

Purpose

Small and Medium-Sized Enterprises (SMEs) share many of the same cyber security needs and challenges as larger organisations but often have significantly less knowledge and capability to deal with them. A fundamental initial issue can be locating relevant information, with the natural route for SMEs seeking and referring to related guidance found online. This can be challenging considering the volume and variety of sources that can consequently be located. This article explores the barriers to cyber security adoption faced by SMEs potentially stemming from the coverage, completeness and clarity of online guidance documents.

Design/methodology/approach

An assessment of over 30 UK-based guidance sources with two subsequent semi-structured interview-based studies with 24 participants (12 providers and 12 SMEs).

Findings

Results from the assessment reveal that there is significant diversity in the materials that SMEs may be presented with, potentially leading to inconsistent and ill-informed decision-making and confusion. Findings from subsequent interviews highlight the impact of guidance related vectors when implementing advice. These aspects are exacerbated by SMEs' reactive needs, internal limitations and awareness of cyber security – hindering their ability to act competently in the context of cyber security.

Originality/value

This contributes to a limited amount of research of how SMEs seek support for cyber security and the effectiveness and impact of online guidance. It also explores this theme from the viewpoint of SMEs and providers in tandem to offer a deeper understanding of security adoption through their lived experiences.

Keywords: Cyber Security, Guidance, Small Business, SME, SMB, Support

1 Introduction

In something of an ironic contradiction, Small and Medium-Sized Enterprises (SMEs) will typically account for the largest population of businesses in a given country and collectively make the biggest contribution to its economy. In the UK, for example, small businesses represent 99.9% of 5.6 million businesses, account for three-fifths of employment and approximately half the turnover in the private sector (FSB, 2023). In this context it is easy to appreciate why the resilience of SMEs is therefore an important aspect to safeguard, and for most this will include attention to the cyber perspective (recognising that SMEs are often as dependent upon digital technology and online connectivity as their larger counterparts). However, in comparison to larger organisations, SMEs are often significantly less well-positioned to take care of their own cyber security needs. Moreover, this limitation is not only in terms of being able to act, but also in relation to understanding the issue in the first instance.

In practice, while they are often labelled collectively, SMEs are an extremely varied community, with businesses that may range significantly in size as well as sector and focus. For example, using the commonly accepted classifications of business size, micro businesses are up to 10 employees, small businesses range from 10 to 49, medium are 50 to 249, and anything above this is classed as large (European Union, 2023). This is ultimately a rather large spectrum and can have resulting implications in terms of how the businesses then use and manage IT. For example, while a sole trader may essentially be running their business via a single device, a small business may be dealing with multiple devices across multiple locations. The business size will also affect their likely resourcing to deal with the issues, which in turn may determine whether they are able to turn to external support. As an example, the UK's 2025 Cyber Security Breaches Survey indicates that 44% of businesses have an external cyber security provider (DSIT, 2025). However, the specific figure varies considerably when looking at business size. For micro businesses it is 39%, for small 62% and for medium 68%, before then dropping back to 50% amongst large businesses. The potential explanation here is that as business size increases, they are better placed to engage (and pay for) an external provider, but equally that once the business reaches a certain size, the need for external support decreases (as the business is large enough to warrant its own dedicated staff and matters tend to be taken back in-house). However, this leaves a significant proportion of SMEs – particularly at the smaller end of the scale – appearing to manage cyber security for themselves. This in turn raises the question of whether they are indeed doing it, and how well they are supported to do so. In this context there is also a very clear link to the human aspect, insofar as (in the smaller cases in particular) cyber security decisions will still come down to an individual, and will therefore very much be linked to understanding and awareness at the personal level.

The question of *whether* they are doing it may also depend upon the type of business they are operating. For example, a sole-trader operating as an accountant, working in a regulated sector (financial), may have a better appreciation of their need for cyber security than an 8-person bakery or 12-person real estate agency, but all could be equally dependent upon resilient systems and protected data as part of their business operations. Equally, in any of these scenarios it is easy to imagine them handling the

situation for themselves rather than having a managed provider, and so it is relevant to consider what they would find if they were to seek guidance and support from other available sources.

Following on from the discussion above, the focus of this paper is to investigate and assess the situation based upon an analysis of online resources that SMEs would be likely to encounter. The work is conducted as part of a wider research project that also seeks to extend the support options available, with the current study representing part of the initial work to assess the current position. The next section presents an overview of the parent research project, and section 3 outlines the methodology adopted for the identification and assessment of online sources. Section 4 presents the findings in relation to three key areas of assessment, the implications of which are then discussed in section 5. The current paper is an extended version of the material that originally appeared in Khan et al., (2024). Thus, this is version particularly expands the discussion segment to include findings from two subsequent studies that followed the original submission, as well as further exploration of the initial findings that took place beyond the presentation at the conference. The paper then concludes with a reflection of the results to date and how they are informing the ongoing work within the project.

2 The CyCOS Project

The research is being conducted as part of a 2.5-year project entitled 'Enhancing Cyber Resilience of Small and Medium-sized Enterprises through Cyber Security Communities of Support' (CyCOS; see https://www.cycos.org/.). This is funded by the UK Engineering and Physical Sciences Research Council (EPSRC) and linked to the Research Institute for Sociotechnical Cyber Security (RISCS) (see www.riscs.org.uk). The overall project has two main aims:

- to better understand the cyber security support needs of SMEs, and
- to pilot a new approach that engages them in further supporting each other.

The initial research is assessing the current situation from the perspective of SMEs *seeking* support, and from those *providing* SME-facing advice and support. The SME data collection (conducted via surveys and interviews) seeks to establish their current understanding perceptions and confidence around cyber security, as well as their support needs and awareness and use of existing routes available to them. A parallel phase, and the focus of this paper, focuses on the support routes and sources available to SMEs. This in turn will inform the new contribution of the project, namely the design and pilot of Cyber Security Communities of Support. These aim to offer an additional route by which SMEs can seek and receive support from peer organisations (e.g. in the same locality or sector) and expertise from advisors willing to offer their support and guidance in a community context.

In addition to the core academic team, the project involves collaboration with a range of relevant supporting partners, including the UK Home Office, ISC2, the IASME Consortium, and three regional Cyber Resilience Centres (which exist to support SMEs and third sector organisations and reduce their vulnerability to cybercrime). Amongst

these, IASME is responsible for delivering Cyber Essentials (a UK Government-backed minimum level of cyber security for businesses that the project is using as a reference point for participating SMEs), and ISC2 is contributing access to its Certified in Cybersecurity (CC) training as a means of upskilling of SMEs and advisors participating in the CyCOS pilots.

3 Research Methodology

This section describes key elements of the approach used to identify and then analyse a suitable set of SME-facing guidance sources. It begins by explaining how the sources were identified, and then proceeds to consider the different perspectives from which they were then assessed.

3.1 Identification and classification of guidance sources

The first requirement was to establish a suitable set of guidance materials that interested SMEs themselves would be likely to discover. In order to mirror the likely approach of SMEs in seeking advice and support, this was based upon a series of web-based searches for related guidance, targeting cases in which the guidance was specifically framed to address the SME audience.

The searches were conducted in September and October 2023. In traditional web searching approximately 12 results per page are presented, and previous research has suggested that only one in ten users are likely to progress to the second page of search results (Turner et al., 2021). In this instance, using Google, the results appeared as an 'infinite scroll', automatically populating additional results as users scroll down the page. As such, in order to ensure that the results from each search were inspected thoroughly and relevant pages had the chance to be identified, the first 38 results were examined for each search (i.e. although not a comprehensive analysis of every document available online, this would be a reasonable sample of what SMEs themselves would be likely encounter). Moreover, relevant providers of guidance had a chance to be located via a series of independent searches, and so the actual assessment was based on the first 38 results from *each* of the following (where 'SMB' is an abbreviation for Small and Midsize Businesses which can be used interchangeably for 'SME' or Small and medium-sized enterprises):

- cybersecurity guidance for small businesses
- cybersecurity guidance for small businesses UK
- SME cyber security UK
- SME IT cyber security UK
- how to set up cybersecurity for SME UK
- how to set up cybersecurity for small business UK
- how to set up cybersecurity for SMB UK
- cyber security policy for small business UK
- cyber security tips for small businesses UK
- cyber security tips for medium businesses UK

- how to cyber secure small business UK
- how to cyber secure medium business UK
- cyber security support for SME UK
- cyber security materials to support SME UK
- cyber security support materials for UK SME
- cyber security support for small enterprise UK
- cyber security support for medium enterprise UK

Although this may still not include all the terms that an SME might use, it was considered to be a suitably well-rounded set. In addition, in case a more complex Boolean search formulation was also attempted, in order to determine whether this returned any further results that may have been omitted in the more general search results:

> [("SME" OR "small business" OR "micro business" or "SMB") AND ("Cybersecurity" OR "cyber security" OR "information security" OR "infosec" OR "security") AND ("advice" OR "guide" OR "guidance" OR "recommendations" OR "tips")],

However, this only delivered results comprised of articles and blogs for SMEs until the 38-result cut-off and hence these results were excluded from further consideration.

During the inspection of results from each search, several exclusion criteria were applied in order to focus upon results that were applicable and relevant to the UK SME landscape, and to ensure that the resulting materials were actually presenting 'guidance' (as opposed to broader discussion) and were comparable in terms of format (i.e. text-based resources rather than videos). As such, the following were excluded in the results: adverts and sponsored links; results from outside the UK; guides in non-text format such as videos; articles from Higher Education institutes; content discussing trends, news and statistics but lacking guidance; guides that simply reference or link out to other providers; and sites that only offered information about their cyber security trainings and certifications.

In addition to the sources identified through the web searches, the authors also added some examples based upon other types of providers that it was considered that SMEs may expect to turn to for guidance. This led to the inclusion of some additional sources from Internet Service Providers (ISPs).

The above process resulted in a list of 72 relevant providers/sources, which was then further filtered based upon practical criteria. Specifically, guides that were only accessible through signing up and/or after paying fees (e.g. to purchase a document or for memberships) were excluded on the basis that SMEs with a more casual interest might not commit to registering, or may lack sufficient financial resources to pay for access. This reduced the list to 44 sources, which were then grouped according to seven categories of provider type that were apparent within the set as a whole. These are listed and described in Table 1.

Table 1. Categories of support provider

Provider type	Description
Government (G)	Sources such as government departments and related agencies, whom SMEs may regard as an official source of information.
IT body (B)	Professional and industry bodies in the IT/technology sector, whom SMEs may regard as relevant from their relationship to the technology being protected.
SME body (S)	Organisation representing or supporting the SME community, whom SMEs may already use for guidance and support as more of a peer community.
Insurance (I)	Insurance providers or others linked to this industry, who may offer guidance for those seeking to insure themselves against cyber incidents.
Security vendors (V)	Those selling products and services in the cyber security sector, who may be regarded as having the security-specific advice to follow.
ISP (P)	Internet Service Providers, from whom SMEs may get their online connectivity, and who may be seen as a natural source of advice for related protection.
IT retailers (R)	Those selling the hardware and software products that SMEs may use, and potentially a natural source for customer support.

From the forty-four providers, 13 further entries were removed following examination of the actual linked resources (where, despite initial appearances, no suitable guides were found). This left a final total of 31 sources as inputs to the detailed analysis phase. Again, while this may not be an *exhaustive* capture of the available sources, it is felt to be sufficiently *representative* – covering the most prominent web search results and spanning a range of provider types.

3.2 Analysis of sources

Following the creation of the shortlist of SME-facing online advisory providers, a comparative assessment was carried out to provide insight into the situation for SMEs attempting to support themselves. Since each provider offers numerous guides, we began by selecting one piece of guidance by each provider. This selection was based on: a) choosing a guide that specifically targets SMEs either by virtue of its title or the nature of the site in which it is provided; b) the guide offers advice about a broad range of cyber security topics as opposed to being topic specific; and c) is not largely duplicating or reusing content covered by another provider already in the shortlist (e.g. material from Provider A being referenced, presented or cross-promoted by Provider B). Analysis of the guides for coverage, completeness and clarity was carried out by the author (NK) and independently checked by the second author (SF). In instances where there was disparity in scores or ratings, both authors shared their initial comments from analysis before discussing and agreeing on a final score.

Assessment of *coverage* evaluated topics that were being addressed in the guides, *completeness* was assessed by the depth of the guide itself (which included guiding

SMEs on *how* to be cybersecure such as through actionable steps and providing links to additional resources for further support), and *clarity* assessed the potential for non-technical SMEs to understand and meaningfully engage with the material.

For the consideration of Coverage, it was necessary to have a reference point for the types of topics that would be relevant to cover, which in turn required some decomposition of the cyber security topic space. Rather than devising a bespoke or ad hoc categorisation, the study adopted the categories from the well-established *10 Steps to Cyber Security* from the UK National Cyber Security Centre or 'NCSC' (NCSC, 2021). These are listed in Table 2, with the abbreviations (which are not part of the normal NCSC usage) being introduced for use as part of the later assessment.

Table 2. The 10 Steps to Cyber Security

Risk Management (RM)	Identity and Access Management (IA)
Engagement and Training (ET)	Data Security (DS)
Asset Management (AM)	Logging and Monitoring (LM)
Architecture and Configuration (AC)	Incident Management (IM)
Vulnerability Management (VM)	Supply Chain Security (SC)

Although the 10 Steps are ostensibly aimed at medium and large organisations in terms of the actual guidance, the constituent themes can still be clearly seen to have some relevance in the SME context (the possible exception is Supply Chain Security, although even here the SME could certainly be *part of* a supply chain, even if it does not formally perceive itself to have one). Additionally, two further categories were added to the assessment of coverage - namely Threats (T) and Other (O) - in order to record whether the guidance covered details of cyber threats that SMEs should be concerned about, and if any points of guidance sat outside of the 10 Steps topic areas.

The Completeness of the guidance was determined based upon subjective assessment of the depth of guidance (as judged by the research team, and rated low, medium or high), accompanied by objective measures related to the length (word count) of the guide and the number of links out to other sources for support.

The assessment of Clarity was based upon a wider range of characteristics, including the level of information presented to users and the assumptions made about their ability to understand and interpret it. Specifically, this rated (on a low-medium-high scale) the extent to which the source provided scene-setting on cyber security (i.e. what it is and why it matters to SMEs), the nature of related threats, and whether the focus of the material stayed clearly on-topic. Then in terms of considering the audience, the perceived levels of IT and cyber security knowledge required to follow the guidance were each rated (this time in terms of beginner, intermediate and advanced levels). Finally, low-to-high ratings were then applied to whether the presented information offered Manageable/easy-to-follow steps, and Yes/No ratings were applied to whether the guidance was considered to describe what 'success' would look like (i.e. to enable the SME to understand what to expect as a positive outcome).

The next section discusses the findings from this comparative assessment of the 31 shortlisted SME-facing online advisory providers across 12 categories. This is with an aim to shed light on the situation for SMEs in attempting to support themselves to

establish or improve their cyber security posture. It should be noted that while the sources are categorised by origin, the specific provider identities are anonymised, as the intention of the work is not to indirectly highlight or criticise any of the sources.

4 Findings

The web search revealed the magnitude of guidance available to SMEs. The likely challenge is therefore not to *find* information, but judging whether it provides support in a manner that the target audience would find understandable and actionable.

Before going into the assessments in the coverage, completeness and clarity, a general statement can be made about the currency of the guidance located. Ten of the sources did not state the date of publication, but of the remainder one was published in 2014, ten between 2015-2020 and five between 2021-2022. This meant that only five guides were published in the year that the assessment was being undertaken (2023).

4.1 Coverage

The coverage of topics varies considerably across guides, with the result that (across the set of resources) some sources have more coverage than others and some topics are more likely to receive attention. This is illustrated in Table 3, where it is immediately notable that no topic was deemed to be covered by all sources, and no sources cover all topics (note that the table uses the abbreviations of the provider types from Table 1 and the topic areas from the 10 Steps to Cyber Security, previously presented in Table 2).

Table 3. Comparison table of each guide for its coverage

Provider /Source	Type	RM	ET	AM	AC	VM	IA	DS	LM	IM	SC	T	O
1	G			✓	✓		✓	✓				✓	
2	G		✓	✓	✓	✓	✓	✓				✓	✓
3	G		✓	✓	✓		✓	✓				✓	
4	G		✓		✓	✓		✓	✓			✓	
5	G		✓	✓	✓	✓	✓	✓		✓		✓	
6	B	✓	✓		✓		✓	✓					
7	B		✓		✓	✓	✓	✓		✓		✓	
8	B		✓	✓	✓	✓	✓	✓					
9	B		✓		✓	✓	✓	✓		✓			✓
10	B	✓	✓	✓	✓	✓	✓	✓				✓	✓
11	B			✓	✓	✓	✓	✓					
12	S				✓		✓	✓	✓	✓		✓	
13	S		✓		✓	✓	✓		✓				
14	S		✓	✓	✓	✓	✓	✓		✓			
15	I	✓	✓	✓						✓		✓	
16	I	✓	✓		✓	✓		✓	✓		✓		
17	I	✓	✓	✓	✓		✓	✓	✓				
18	I		✓		✓	✓						✓	
19	V		✓	✓	✓	✓	✓	✓	✓				
20	V	✓			✓	✓	✓	✓					
21	V		✓		✓		✓	✓		✓			
22	V		✓		✓	✓	✓	✓					
23	V		✓		✓		✓	✓					
24	P	✓	✓		✓	✓	✓	✓					
25	P		✓		✓	✓	✓	✓					
26	P		✓		✓								
27	P		✓		✓	✓	✓	✓					
28	R		✓		✓	✓	✓	✓					
29	R		✓		✓	✓	✓		✓				
30	R	✓	✓		✓		✓						✓
31	R				✓	✓	✓						

An accompanying visual summary of the 10 Steps coverage is summarised in Fig. 1. The most well-represented topic proved to be *Architecture and configuration*, which encompasses a number of the technically oriented issues that guidance would tend to talk about (including having up-to-date malware protection, network firewalls, controls

on organisation-owned devices, protecting Wi-Fi networks and use of VPNs). *Identity and access management* was popular as a result of topics such as strong passwords, two step verifications (2SV), and access control being mapped to this step. The equally placed *Engagement and training* category was used to code any advice relating to training, awareness, security policies, policies of use, getting Board buy-in, and creating security culture. For the other categories considered to be represented in more than half of the guides, *Data Security* scored well because it was the category used to map advice around backup, and *Vulnerability management* captured any instances of advice around keeping systems and software updated and patched.

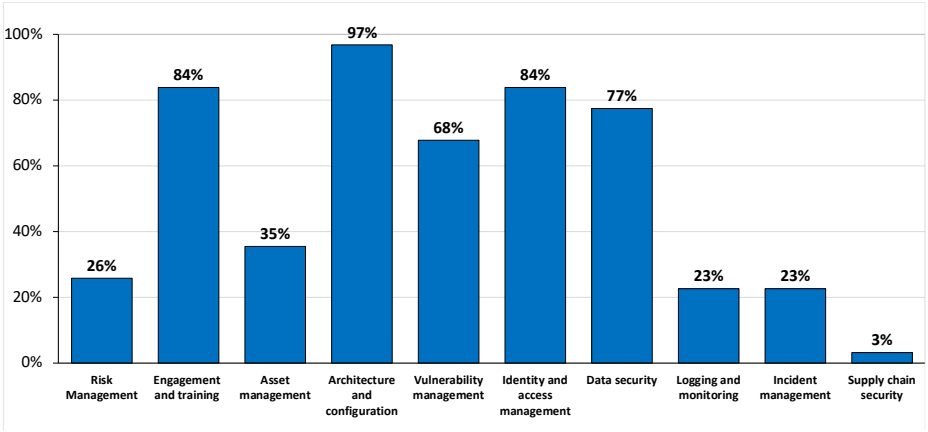

Fig. 1. Frequencies of topic coverage across the guides

At the other end of the scale, the topics receiving the least coverage were *Supply chain security* and *Other* (with the latter including aspects such as physical security of devices and premises and joining cyber security communities for support). Whilst guides often mentioned supply chains, it was typically in the context of other topics. For example, one source mentioned cloud suppliers in the context of backing-up data. Thus, whilst the supply chain is referenced, it is not in the context of how to manage this aspect (which is what the related item in the 10 Steps is referring to). Only one guide was found to provide guidance on vendor security controls and practices as part of its corpus. Overall, and in contrast to others, the lack of attention towards this particular theme from the 10 Steps is perhaps explainable by the fact that SMEs tend to be part of someone else's supply chain rather than having one of their own. However, the paucity of coverage in other themes (e.g. managing assets and incidents) could arguably leave SMEs underprepared and exposed in some areas.

Table 4. Findings relating to completeness and clarity of the guides

	Completeness			Clarity						
Provider	Depth	Word len.	No. links	Def. cyber	Def. threats	Topic focus	Reqs IT knowl.	Reqs cyber knowl.	Easy	Def. success
1	H	3,446	24	L	M	H	B	B	H	N
2	H	3,960	52	H	H	H	I	B	L	N
3	L	669	3	L	L	H	I	B	M	N
4	L	405	6	M	M	H	B	B	M	N
5	M	1,540	32	L	M	H	B	B	H	N
6	H	6,983	81	L	H	H	I	B	L	N
7	L	491	2	L	M	M	I	I	L	N
8	L	239	0	M	M	L	B	B	L	N
9	L	326	1	H	L	L	B	B	L	N
10	H	3,749	17	L	H	H	I	B	H	N
11	H	1,347	33	L	H	H	B	B	H	N
12	M	536	12	H	M	H	B	B	H	N
13	M	683	2	L	M	H	I	B	L	N
14	M	971	4	L	M	H	B	B	H	N
15	L	899	4	L	H	L	B	B	L	N
16	H	960	4	H	H	H	I	B	H	N
17	M	3,462	0	H	H	H	I-A	B	M	N
18	M	679	6	M	H	H	B	B	H	N
19	M	780	0	L	M	H	B	B	L	N
20	L	482	4	H	H	H	B	B	L	N
21	L	322	0	L	L	L	B	B	L	N
22	M	758	7	M	H	H	B	B	H	N
23	M	847	4	M	M	H	B	B	M	N
24	L	335	1	H	L	M	B	B	L	N
25	M	807	5	L	M	M	B	B	H	N
26	L	431	1	M	H	L	B	B	L	N
27	M	978	0	L	M	H	B	B	H	N
28	L	1,297	9	M	M	M	I	B	L	N
29	L	607	5	M	H	H	I-A	B	L	N
30	L	522	0	L	L	H	B	B	L	N
31	L	998	16	L	L	H	B	B	H	N

Key: H=High, M=Medium, L=Low, B=Beginner, I=Intermediate, A=Advanced, N=No

4.2 Completeness

This attribute explored the extent to which guides were able to offer comprehensive advice to their SME audiences for their cyber security needs as standalone documents. The depth of guidance was assessed through analysing the level of detail provided in the advice (i.e. whether the guide provided topic level advice or actionable steps on how to achieve said instructions). Additionally, aspects such as the length of the document and the number of link outs (i.e. pointing to URLs that provided further information or support) were also captured as part of the analysis. The findings are shown in Table 4.

In terms of depth, almost half (45%) of the guides evaluated as 'low', suggesting that they were (for example) name-checking topics of interest without offering tangible details or descriptions of them. Only around a fifth were judged to offer high quality advice, which included details of how to enact the advice being given to audiences.

It is notable that the independently made ratings of depth tend to track with the length of the guides and the number of links out that they provide. It can be seen that the length varied significantly overall, from 239 to 6,983 words, but with three quarters coming in at below 1,000 words. The number of link outs to other sources for support was also highly varied, with six guides offering none at all and five offering in excess of twenty. The average was 11, but this is rather skewed by the source with 81 links. In general, the presence of links to other sources can be regarded as a positive, as it suggests that guides are trying to direct readers to other sources of support (which in turn may offer more specific and detailed guidance that would not be appropriate to offer in a general resource).

4.3 Clarity

Clarity also varied between providers. Half of the guidance documents did not provide any definition of cyber security. However, ~80% did something tangible in terms of presenting information about related threats, out of which ~40% were judged to be offering high quality of information. In terms of the presentation of the material, two thirds of the guides were written in layperson terms that did not require the audience to have IT knowledge, and only two guides were judged to be verging into requiring an advanced knowledge here. This meant that most guidance documents did not use jargon or technical terms that might confuse a non-specialist audience. Similarly, all but one of the guides were written from the beginner's perspective in terms of expecting no prior cyber security knowledge. However, half of the guides did not provide clear, easy steps for readers themselves to follow and in most instances stated that the audience would need the assistance of an IT specialist to perform the recommended steps. Alternatively, steps involved advice on purchasing off-the-shelf security products. Finally, none of the guides shared what the audience would expect to see if steps were followed correctly. This lack of detail regarding successful completion of steps suggests that audiences may not know if they had correctly implemented cyber security defences after following the guidance.

5 Discussion

The varying findings across the differing dimensions of coverage, completeness and clarity can in turn have implications for the SMEs who may locate and seek to use the available guidance. Firstly, and perhaps fundamentally, the spread of information across topics and the variance in the nature of the guides themselves may cause confusion, frustration and discouragement for an SME looking for cyber security advice and support and, adversely affect their cyber security journey. Research by Redmiles et al. (2020) showed similar findings of SMEs struggling to prioritise cyber security advice that is somewhat comprehensible and subsequently actionable which can then alienate SMEs in their journey. In line with our findings for 'completeness' and 'clarity', accessibility of information found in guidance that is being provided to SMEs was found to be a notable area (Wilson & McDonald, 2024) for improving their subsequent engagement with cyber security. Additionally, with some of the guides being relatively dated, SMEs may encounter sources offering a less up-to-date view of the challenges they face and may be missing the most recent or most appropriate recommendations. For instance, the most well represented topic in the 'coverage' theme i.e. Architecture and configuration, can include advice which might be outdated due to technological advancements since the time the guide was published.

There are numerous providers offering SME-facing guidance and some have various guides available on their websites. Guides are diverse in their nature. For example, they can be holistic or topic-specific, and based on personal or organisational contexts. This variation is interesting as SMEs would need to know the topic area their challenge would fall within. Identification of topic areas that can be beneficial to a specific SME in their context would demand the use of limited resources and require a heightened situational awareness to encourage proactive implementation of defences (Renaud & Ophoff, 2021a). Even if the topic area is known, it would not circumnavigate the challenges discussed earlier with the coverage and completeness of advice to assist SMEs in their cyber security journey to secure themselves (Neil et al., 2021). Additionally, advice provided for personal contexts might not be suitable for its application to complex, diverse and dynamic organisational contexts that can have legal ramifications for instance, parental control locks to safeguard children from harmful content would not be appropriate in work settings for employees accessing unsafe or social networking websites. Furthermore, in some cases, the focus can change within the website without being obvious that this is the case. For instance, when advising on online safety and security for businesses, one source then linked through into the 'personal user' section of its site without it being obvious to the user who might (at least initially) assume they were still reading business-facing guidance. A similar situation exists with a number of providers and could result in SMEs selecting an inappropriate guide for their needs.

More generally, some providers made it difficult to locate content that SMEs could use when discovering cyber security advice and support suited to their needs. While this would not be the intention of the provider offering guides, the lack of site indexes and insufficient or imprecise search features on their websites made the discovery of relevant content arduous. In some instances, relevant guides were only located by

following bread-crumb trails that emerged as part of the guide discovering journey. For instance, recommendations made by the website through prompts such as 'You may also like' led to a suitable result that was not obvious from original lists or search results. Aside from accessibility to appropriate guides on websites, there is emerging evidence for SMEs to have a transparent and trusting relationship with providers to provide them tailored support, equip them to understand and overcome cyber security related challenges and building communities of support (Rawindaran et al., 2023).

Following the work on this study (Khan et al., 2024), further related research was conducted to develop an understanding of SME cyber security related support needs. The first investigation examined these support needs through the lived experience of providers which potentially stem from the variance in the coverage, completeness and clarity found in online resources. The second concurrent research study complimented the first investigation through exploring SME perspectives that might influence their cyber security posture. Three primary aims of the first study were as follows: 1) to investigate the different types of support offered by providers in their natural contexts (Malterud, 2001); 2) the topics and circumstances under which support is sought and 3) the extent to which the support is believed to be effective by providers, challenges encountered, and lessons learnt. The second study aimed to understand factors that influence whether SMEs access resources to reduce their cyber security risk (Alahmari & Duncan, 2021). A qualitative approach was adopted by the first study which utilised semi-structured interviews to gain a nuanced understanding of lived experiences of providers which encompass sensitive issues inherent to the cyber security domain (Adams, 2015). A qualitative approach was also utilised for the second study through semi-structured interviews as it offered an opportunity for SMEs to outline why SMEs may (or may not) access resources to improve their cyber security (Renaud & Ophoff, 2021b). The study was approved by the School of Computer Science Research Ethics Committee at the University of Nottingham for the provider interviews, and Queen Mary University of London ethics committee for the SME interviews. In both cases, participants were informed of the aims and objectives of the studies and informed consent was acquired before their participation. Participants were also debriefed at the end of their participation and were assured of their right to withdraw at any point.

A total of 24 participants from across the UK were interviewed as part of both the studies (12 providers and 12 SMEs). For the first study this sample size was deemed to be suitable due to the appropriateness of data offered by participants due to their designations (O'reilly & Parker, 2013) and the data reaching saturation during the interview stage (Bekele & Ago, 2022). Table 5 shows provider participant designations and the nature of their respective organisations. Provider participants were recruited through snowball sampling from the professional networks of the authors. Selection criteria included participants' ability to provide relevant data based on their roles at suitable organisations. This meant individuals were deemed as well suited to the overarching aims of this study if they held positions that allowed them to have an oversight of their organisational efforts and organisations had a dedicated team or department offering cyber security support to SMEs. Similarly, for the second study 12 participants were appropriate. In previous qualitative research studies where approximately 12 participants were interviewed, five to six in-depth interviews

produced the majority of new data, and approximately 85% of new findings were identified within the first 10 interviews (Guest et al., 2006; Robinson, 2014). SME participants were key stakeholders in relevant sized organisations (such as owners, employees or experts in cyber security) and belonged to various sectors. Table 6 shows the size of organisations and their respective sectors of operation. SME participants were recruited through a previous study where they expressed an interest to partake in subsequent research. To safeguard provider participants' anonymity whilst demonstrating the significance of findings, the following terms are deployed: 'few' indicates 3 participants or less; 'several' to indicate 4 – 7 participants; 'many' to indicate 8 – 11 participants; and 'all' to indicate all 12 participants (Braun & Clarke, 2021a).

Semi-structured interviews generated approximately 7 hours of data from the provider interviews and approximately 8 hours of data from SME interviews. Data was transcribed verbatim and anonymised to safeguard confidentiality, with participants from both studies referred to as P1, P2 and so on (for providers) and SME P1, SME P2 and so on (for SMEs). Template analysis (King, 2012) was applied to provider interview data to uncover findings. This included a top-down approach through the use of a template containing broad parent and child themes before proceeding with a bottom-up approach to update the initial template through a grounded theory approach (Glaser & Strauss, 2017; Muller & Kogan, 2012). The utilisation of template analysis allowed efficiency and flexibility to the coding structure compared to other approaches (Spiers & Smith, 2019). Subsequently, constant comparison method (Hoda et al., 2010) was used to ensure the individuality of the codes through comparison within and across transcripts until reaching data saturation prior to commencing analysis. Data from the SME study was analysed through thematic analysis to identify patterns within the data (Braun & Clarke, 2021b). This method was suitable for the exploratory nature of this study as it served the purpose of capturing discussions around the overarching themes of the data collected (Braun & Clarke, 2021c).

Table 5. Provider participant designations and nature of organisations

No.	Job Title	Description of Organisation
P1	Chief Executive Officer	Provide information and assistance related to security, technologies and operation of businesses and/or consumer rights
P2	Deputy Head of Insurance	Provide information and assistance related to security, technologies and operation of businesses and/or consumer rights
P3	Senior Manager	Provide cyber security support to SMEs in their capacity as a 'client' to their supply-chain
P4	Head of Department	UK Government department or body
P5	Product Leader	Provide cyber security insurance
P6	Chief Solutions Architect	Provide security education or defensive software to SMEs
P7	Director	Provide security education or defensive software to SMEs
P8	Associate	Provide security education or defensive software to SMEs
P9	Managing Director	Dedicated, not-for-profit organisations that work to further national strategic objectives
P10	Chief Executive Officer	Dedicated, not-for-profit organisations that work to further national strategic objectives
P11	Head of Cyber Security	Dedicated, not-for-profit organisations that work to further national strategic objectives
P12	Cyber Security Consultant	Provide security education or defensive software to SMEs

Table 6. SME participant size of organisation and sector of operations

Participant	Sector	Number of employees
Participant 1	Healthcare	Sole trader
Participant 2	IT and certifications	5 employees
Participant 3	Mental health	9 employees
Participant 4	Consultancy	10 employees
Participant 5	Corporate travel management	50 employees
Participant 6	Telecoms	10 employees
Participant 7	IT services	100 employees
Participant 8	Logistics	160 employees
Participant 9	Software development	13 employees
Participant 10	Data protection advisor	51 employees
Participant 11	Technology	10 employees
Participant 12	Security	Sole Trader

Many providers shared the impact of language and messaging used in cyber security content. This shows potential evidence that the language used and messaging that is chosen to communicate the importance of cyber security can result in SMEs being confused, overwhelmed and, victimised.

> '*Some of the language around cyber security and cyber fraud is very negative and damaging. It basically means you've been tricked, you've been scammed, you've been fooled, and so you're made it feel stupid if you've "fallen" for a trick from a cybercriminal*' – P9
> '*The advice and support coming out, that's very cyber related, and then we've got a business community saying, 'I don't see how this fits''* – P10

Many SMEs also believed that language and messaging were important factors for their adoption of cyber security. Additionally, SME participants shared the belief that support provided (through various mediums) was generic in its nature and not completely relevant to their organisational contexts. SME participants were of the view that to have relevant and specific advice, there also needed to be a level of engagement and interaction between the SME and the provider.

> '*They're not sitting where you and I are actually looking at exactly what it is that we need to do. It can only be at a generic level. To get meaningful, relevant advice you either have to distillate yourself, talk to peers, read online, you know, vender websites, that type of thing, reaching out to them*' – SME P5
> '*The online course that I help with is a basic introduction to data protection for small businesses. It's 12 modules and each module you go through lots of steps and it's the usual online training thing… You know, 'Bill is a hairdresser who also does this'… in some instances it's too simplistic and could put people off. It doesn't say, 'this is what you should do' it's 'you've got the knowledge, it's up to you now"* – SME P10

Several providers emphasised the need to have technical skills to be able to help SMEs with their cyber security which can range from beginner to advanced levels. This variance in provider abilities is believed to be due to two aspects: 1) Being able to understand technical terms used in the domain and subsequently present in guidance documents to effectively advice SMEs, and 2) The umbrella term of 'SME' including a varying audience and subsequently a varying degree of technical requirements for solutions depending on their architecture. The need for providers to have technical knowledge showcases the limitations and challenges faced by guidance documents to become accessible to lay-persons and avoid alienation i.e. being able to provide clarity in documents without the use of jargon whilst providing actionable steps that SMEs can deploy to improve their cyber security posture.

> '*You need to be able to understand the cyber stuff. You'll need to have a technical understanding of some of the terminology*' – P10

'*The biggest challenge is how do you get those messages to those individuals in such a way that a) they will take notice, [b)] that they understand it, and [c)] then they can do something about it*' – P1

The need for technical knowledge was evident in the discussions with SMEs, who acknowledged that they did not understand many of the terms within cyber security, and consequently were unsure of where to go for support. SMEs felt that the technical language involved could put them off in seeking support and could mean they find it difficult to know where to go, merely because of this lack of knowledge.

'*I think that there's a whole education piece out there and it always amazes me in some ways. I don't understand the jargon. I don't understand what it is. I don't want to know*' – SME P1
'*I look at the security of my systems and looking at my domain, that's the part I don't really understand and I don't have any support on it. I phoned the people that we've got a domain through and they can't help me with all of it*' – SME P3

Furthermore, many providers shared that it was essential to be able to communicate technical knowledge into a format that can be comprehensible to a generalist audience in order to provide effective support. With the variation between the broad term of SMEs set aside, providers highlighted the variance in abilities within an organisation that can change between designations, experience levels and backgrounds of individuals. This can pose a new challenge for written guides that are generally aimed at SMEs but might not acknowledge the dynamic nature of individuals and varying abilities within them.

'*Our job is to try and demystify cybersecurity and to try to speak English (layperson terms) and I'm not overly technical to these (SME) organisations*' – P4
'*There are some clients which would surprise you, in terms of their knowledge, definitely. But I'd say generally, particularly for smaller-end customers, you will see very, very limited knowledge*' – P5
'*The company we're working with just now is a security focused start-up so, they are relatively switched on. I've worked with other companies in the past, they were really good at the tech side of things, but they didn't really think about [the] security at all. And then there's been a mix in between [of the two examples above]*' – P3

Whilst the circumstances under which support is sought varies, many SME participants described particular events as being a catalyst for them to seek support. Some of these events were related to experiencing a cyber security incident or breach themselves or the incident or breach occurring within a related organisation, such as

one that was in their own industry. These events brought the focus of cyber security to the forefront of their day-to-day activities.

> ‘W*e had an episode (with our) email being spoofed. These are moments in time that it comes into vision and we go, ‘Okay, what did you do? Does it pose an immediate threat, or is there a bigger threat behind that?”* – SME P4
> ‘*If I get an email to say there's some particular country that's targeting the UK, I will update everybody on that and say this is what you need to be aware of*’ – SME P3
> ‘*Until quite recently, there wasn't much focus on security, but I think because of those reasons our industry has become a target. There's been some quite high-profile ransomware attacks on [named sector] companies and that has definitely caused us to pay a lot more attention to it*’ – SME P8

This sentiment was echoed by many providers who shared that SMEs tend to reach out for cyber security support reactively i.e. following an incident, if they believe they can be susceptible to an attack, to request training or if it is required for compliance. This results in SMEs seeking very specific guidance that is suited to their unique needs or digital architecture and assets. This need is coupled with low general knowledge levels about this domain that potentially results in confusion of identifying suitable subsequent steps they need to undertake or identify guidance that is most appropriate for their circumstances.

> ‘*They (SMEs) would typically come to us if they've seen a threat or, something that's occurred. They might have had an incident like a phishing incident or something along those lines. And then from there we try and support them with that*’ – P12
> ‘*We get contacted by our e-mail account quite frequently. But normally we will get questions when it's too late*’ – P4
> ‘*(An SME) just rung me up because they were undergoing some kind of breach or hacker live as they called me… Quite often, certainly with the SMEs, it's off the back of an incident*’ – P7

Low levels of knowledge amongst SMEs is reflected through the poor baseline cyber hygiene present in SMEs which was an aspect discussed by many providers.

> ‘*You are going to talk to somebody who struggles sometimes to update their operating systems. If you tell them to update, they would be like, ‘What? How do I?” you know, that is the low-level stuff*’ – P6
> ‘*When I talk to people in in the SME world, their knowledge is considered to be quite basic… some of them haven't even got a clue about keeping their social media profiles safe. It really is quite basic*’ – P8

'*They [SMEs] have just gone off and they've got 15 Macs or 15 PCs, they've got a Google or M365 environment, and they've sort of set it up themselves and hope they've done it right*' – P7

Additionally, as part of these discussions providers shared the lack of knowledge places an unfair burden on SMEs to make informed decisions about their cyber security, especially if it is coupled with strained or scarce resources such as time, money, skilled labour and expertise.

'*(SMEs will say) 'I'd buy Apple, but I can't afford Apple. You'll pay premium for that [device]'… So, some people would look at it from a longevity and sustainability point of view, that they can project their fixed payments… Finances and knowledge levels right at the beginning of projects, your average small business owner would never possess that much knowledge, because then they wouldn't be the Florist or the Baker [instead], they'd be a cyber security expert*' – P11

'*For businesses in regions that are not specialised, it can be hard. If you live in London or Edinburgh, Bristol, it's probably relatively easy to get to security person… They (SMEs) don't have access to the people, they don't have the funding to pay for people, they don't have the funding to pay for the tools, that's what causes a lot of the problems*' – P3

This scarcity of resources was also reflected in SME participants, who highlighted a lack of resources within their organisations to seek cyber security support. Although many SMEs have an aspiration to pursue support that could enhance their security, many are aware that this will result in increased time and money, which SMEs may not have access to.

'*We're not going down the Cyber Advisor route lightly because it's time consuming, means I've got to do some studying, and this isn't a cheap thing to do. We want to do it for the whole business which is going to cost a fortune*' – SME P6

'*The thing which has bothered me since I started running my own business is backup. I want to stay cost effective. Something that I think is effective and at a reasonable price. I don't necessarily think that throwing money into cloud solutions is a reasonable price for what you get* ' – SME P12

SMEs also highlighted the scarcity of resources that pertain to availability of individuals with technical expertise. This results in SMEs not being able to identify cyber security related problems that need to be solved and consequently ways to solve them. Some larger organisations within the SMEs umbrella might employ a dedicated IT professional who has this required level of expertise due to advantages associated to their size. However, for organisations that are unable to do so, this responsibility falls on the owner or founder of the SME, or an employee who has operational responsibilities, of which cyber security is one of many.

'*Because we are only 10 employees, we're in the awkward middle where we don't have a dedicated IT function because we're not quite big enough to have one. So, in terms of internally, it would probably fall to me as the decision maker*' – SME P4
'*In terms of who would I go to talk about this (security), I wouldn't know. Probably the best thing I would be able to do would be go to a managed service provider, some IT outsourcing company that specialises in small-medium businesses*' – SME P6

All provider participants echoed the above sentiment, believing that SMEs are generally unaware of cyber security related issues which can potentially result from competing operational priorities faced by organisations without relevant expertise. Subsequently, SMEs are unaware of the aspects they need help with. Furthermore, they are largely unaware of the routes to receive help which influences their ability to act competently in the context of cyber security.

'*They've (SMEs) got no idea. They're working with insecure websites… they don't really know how to save and protect themselves. They've got no idea where to go for help to improve their protection*' – P9
'*Certainly, mid-size [and] larger firms probably have the resources. But if you're a smaller business, you don't have access to all those resources. So, they're response is, "Is it going to happen to me? What do I need to do about this? Well, my MSP does all of that" Because they also get really flummoxed by the jargon, the IT security jargon, it makes cyber security very remote to a lot of people*' – P2

In addition to the lack of knowledge and resource adversities faced by SMEs, several providers acknowledged the importance of being skilled to efficiently locate suitable guidance documents or appropriate services themselves.

'*There's a plethora stuff out there. But as long as you know where it is and you're telling somebody to do the right thing, to look at a certain bit of advice or guidance released by the government, then that's fine*' – P9
'*Identifying what's where and who needs to do it, is very key*' – P7

It was clear that SMEs found it difficult to locate suitable guidance or were left with further questions on what they should do next. SMEs were then not totally clear on where they could find additional resources that would help them beyond what they had initially identified.

'*The main place that I go to is the NCSC website. Their website is quite straightforward and I can follow most of it. But when it comes to them saying, "MTLS TLS settings within the domain" and then they're saying, "create a sub domain" and I'm thinking, 'How do I do that?"* – SME P3

> ‘*There are tools that are easily available, where you put your IP or email address in. And it says “Your email account is okay apart from it's missing these things that you ought to look at, like SMTP, you might be susceptible to these kinds of things”. And I look at that and say, ‘What the hell are those?’. I go and Google those, bring them up, find out what all these lists of letters and things mean, and then I've got to say, ‘Right, does that actually apply to us?’*” – SME P10

Findings discussed above further highlight the point made in the initial publication (Khan et al., 2024) about the spread of information across topic areas between guides and the variant nature of guides that are available to SMEs. These variances require providers, who are rehearsed in the domain of cyber security, to emphasise the importance of being able to locate suitable documents themselves in order to assist SMEs. Thus, making information easily accessible to SMEs through improving aspects discussed in the findings for ‘clarity’ and ‘completeness’ of guides can potentially improve their engagement with this domain.

With a lack of knowledge and limited resources, SMEs arguably would not be able to make informed decisions or be able to identify which resources to select when information is spread across guides nor understand the importance of selecting an appropriate and up-to-date guidance document that is suited to their needs. With a fundamental lack of knowledge about this domain, an independent attempt to improve their posture or safeguard themselves might result in SMEs being further removed and more confused than when they started out. Herein lies two challenges for guidance documents that offer cyber security support for SMEs: firstly, to offer guides that consider all three elements of coverage, clarity and completeness to aid SMEs in their selection of appropriate guidance and to compensate for any limitations in knowledge. Secondly, to acknowledge the variance between micro, small and medium sized enterprises, the nuanced differences between similar sized organisations and to acknowledge the dynamic nature of individuals and their abilities within organisations who are the target audience and benefactors of these documents. Overcoming these challenges can potentially help better support SMEs in their journey to become cyber secure.

6 Conclusions

The most notable finding from the study was the variation in coverage, with the potential risk that SMEs may form a very different interpretation of what cyber security *means* (and involves) depending upon the reference point they have worked from. The accompanying issues – such as whether the resulting guidance is then framed in an accessible manner and covered in sufficient depth – then represent further challenges that may ultimately frustrate SMEs’ efforts and good intentions.

It is worth noting that while materials in written format were the focus of this study, relevant SME cyber security guidance can also be offered in a range of other formats, including infographics, posters, recorded webinars, and podcasts. As such, some

content will have been implicitly excluded from this analysis that might nonetheless provide useful cyber security content and guidance. Most notable, however, is that some SMEs will seek guidance in other ways, and will approach potential sources directly with their questions and concerns. As the authors are experts in this field the assessment of guides can represent a higher threshold of technical knowledge required when interpreted by a non-expert or laypersons. However, predetermined measures were used to analyse whether the guide required IT or cyber security knowledge to represent laypersons understanding. For instance, the use of jargon or technical terms that might confuse a non-specialist audience or noting when the guide self-declared the preexisting need for such knowledge to benefit from the guidance provided therein.

The assessment of online sources was followed by two concurrent research studies which adopted a qualitative approach through semi-structured interviews. The first involved 12 support providers whilst the second study engaged 12 SMEs (n=24). Findings reveal SMEs can feel confused, overwhelmed and victimised due to the language and messaging used in cyber security related content. This language and messaging barrier, alongside generic advice and the lack of engagement, are factors that adversely affect the adoption of cyber security amongst SMEs. Providers shared their own need of requiring technical skills to be able to effectively locate and utilise relevant guidance documents when assisting SMEs. This is further evidenced in SME discussions which highlight the lack of knowledge can hinder their efforts in getting the support that might be crucial to their security, especially if support is being sought reactively i.e. following an incident or a breach. Improving the clarity aspect of guidance documents can aid in SMEs' accessibility to knowledge and subsequently improve their cyber security posture. Improvement of this aspect would require enhanced communication and acknowledgement of the variation in abilities, experience levels, backgrounds, resources and architectures within and between SMEs. It is worth noting that challenges arising from resources include time, money, and access and identification of suitable expertise – all aspects that compete with the prioritisation and adoption of cyber security in SMEs. Thus, efforts to improve clarity within guidance documents would ultimately help ease the undue burden placed on SMEs for making informed decisions and reducing the demand on limited resources to assist SMEs in improving their cyber security posture.

Whilst a diverse and appropriate set of provider organisations and SMEs participated in the two research studies, it is important to note that snowball sampling can limit the variety of participants and the generalisability of findings. As participant views are informed by their organisational contexts, sectors of operation and societal norms, this can limit the applicability of findings to organisations in other countries. Finally, views shared by participants can differ from other stakeholders within their organisations due to their designations, nature of work, and involvement in day-to-day operations when delivering support.

The ongoing work within the project will seek data collection in a more longitudinal manner, with data being collected from both SMEs and providers as part of their support journeys (i.e. logging individual instances of support activity as they occur and capturing it from both perspectives). From this, the intention is to build up a series of more comprehensive picture of what the support experiences look like, where support

is and is not sought, and where it is effective. This in turn will help to establish the foundations for the later work to be conducted in relation to designing and piloting the planned communities of support.

Acknowledgments. The research is conducted as part of the project 'Enhancing Cyber Resilience of Small and Medium-sized Enterprises through Cyber Security Communities of Support', funded by the Engineering and Physical Sciences Research Council (grant reference EP/X037282/1) and linked to the Research Institute for Sociotechnical Cyber Security.

References

1. FSB: "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, last accessed 2024/5/5 (2023).
2. European Commission: Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises. Official Journal L 124 , 20/05/2003 P. 0036 - 0041. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003H0361, last accessed 2024/5/5 (2023)
3. CSBS: *Cyber Security Breaches Survey 2024*. Department for Science, Innovation and Technology. 10 April 2025. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025 , last accessed 2025/4/11 (2025)
4. Turner, S., Nurse, J.R.C., Li, S.: When Googling it doesn't work: The challenge of finding security advice for smart home devices. Human Aspects of Information Security and Assurance. HAISA 2021. IFIP Advances in Information and Communication Technology, vol 613. Springer, Cham. https://doi.org/10.1007/978-3-030-81111-2_10 (2021)
5. NCSC: "10 Steps to Cyber Security", National Cyber Security Centre, 11 May 2021. https://www.ncsc.gov.uk/collection/10-steps, last accessed 2024/5/5 (2021)
6. Redmiles, E.M., Warford, N., Jayanti A., Koneru, A., Morales, M., Stevens, R., Mazurek, M.L.: A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web. 29th USENIX Security Symposium (USENIX Security 20) (pp. 89-108). (2020)
7. Wilson, M., McDonald, S.: One size does not fit all: exploring the cybersecurity perspectives and engagement preferences of UK-Based small businesses. Information Security Journal: A Global Perspective, 1-35 (2024)
8. Renaud, K., Ophoff, J.: 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 (2021a)
9. Neil, L., Bouma-Sims, E., Lafontaine, E., Acar, Y., Reaves, B.: Investigating Web Service Account Remediation Advice. Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021) (pp. 359-376) (2021)
10. Rawindaran, N., Jayal, A., Prakash, E., Hewage, C.: 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 (2023)
11. Khan, N., Furnell, S., Bada, M., Nurse, J.R.C., & Rand, M. (2024, July). Assessing Cyber Security Support for Small and Medium-Sized Enterprises. In International Symposium on

Human Aspects of Information Security and Assurance (pp. 148-162). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-72559-3_11 (2024)
12. Malterud, K. (2001). Qualitative research: standards, challenges, and guidelines. The lancet, 358(9280), 483-488. https://doi.org/10.1016/S0140-6736(01)05627-6 (2001)
13. Adams, W. C. (2015). Conducting semi-structured interviews. Handbook of practical program evaluation, 492-505. https://doi.org/10.1002/9781119171386.ch19 (2015)
14. O'reilly, M., & Parker, N. (2013). 'Unsatisfactory Saturation': a critical exploration of the notion of saturated sample sizes in qualitative research. Qualitative research, 13(2), 190-197. https://doi.org/10.1177/1468794112446106 (2013)
15. Bekele, W. B., & Ago, F. Y. (2022). Sample size for interview in qualitative research in social sciences: A guide to novice researchers. Research in Educational Policy and Management, 4(1), 42-50. https://doi.org/10.46303/repam.2022.3 (2022)
16. Braun, V., & Clarke, V. (2021). Thematic analysis: a practical guide. Sage Publications
17. King, N. (2012). Doing template analysis. Qualitative organizational research: Core methods and current challenges, 426, 426-450. Sage Publications Ltd
18. Glaser, B., & Strauss, A. (2017). Discovery of grounded theory: Strategies for qualitative research. Routledge. https://doi.org/10.4324/9780203793206 (2017)
19. Muller, M. J., & Kogan, S. (2012). Grounded theory method in human-computer interaction and computer-supported cooperative work. The Human Computer Interaction Handbook (3 ed.), Julie A. Jacko (Ed.). CRC Press, Boca Raton, FL, 1003-1024.
20. Spiers, J., & Smith, J. A. (2019). Interpretative phenomenological analysis. SAGE Publications Ltd
21. Hoda, R., Noble, J., & Marshall, S. (2010). Using grounded theory to study the human aspects of software engineering. In Human Aspects of Software Engineering (pp. 1-2). https://doi.org/10.1145/1938595.1938605 (2010)
22. Alahmari, A. & Duncan, R. A. (2021). Investigating potential barriers to cybersecurity risk management investment in SMEs. In 2021 13th International Conference on Elec-tronics, Computers and Artificial Intelligence (ECAI) (pp. 1-6). IEEE
23. Renaud K & Ophoff J (2021b). What is Preventing UK SMEs from taking Cyber Security Precautions? Retrieved 1st November 2024. Available from: https://www.muster.scot/docs/MUSTER_White_Paper.pdf
24. Guest, G., Bunce, A., & Johnson, J. (2006). How Many Interviews Are Enough? An Experiment with Data Saturation and Variability. SAGE Journals, 59-82
25. Robinson OC (2014) Sampling in interview-based qualitative research: A theoretical and practical guide. Qualitative Research in Psychology 11(1): 25–41
26. Braun, V. and Clarke, V. (2021b) One size fits all? What counts as quality practice in (reflexive) thematic analysis? Qualitative Research in Psychology, 18, 328–352
27. Braun, V. and Clarke, V. (2023) Toward good practice in thematic analysis: avoiding common problems and becoming a knowing researcher. International Journal of Transgender Health, 24, 1–6