Investigating the experiences of providing cyber security support to small- and medium-sized enterprises

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

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

{steven.furnell; neeshe.khan1}@nottingham.ac.uk; {m.bada; m.rand} @qmul.ac.uk; j.r.c.nurse@kent.ac.uk

Abstract:

Small- and Medium-Sized Enterprises or SMEs comprise of 99.9% of all businesses in the UK and make a significant contribution the overall economy. In UK's path to digitalisation, ensuring the cyber security and resilience of SMEs becomes an integral element that must be adequately safeguarded to protect national interests. Despite playing a crucial role, there is limited research on SMEs adopting cyber security practices, becoming cyber secure or improving their resilience to attacks. To examine this journey, a qualitative study was designed to learn from the experiences of organisations that provide cyber security advice or solutions. The three aims of the study were to: 1) understand the various types of support offered by providers; 2) topics for which support is sought and the circumstances that trigger the need for assistance; and 3) the perceived effectiveness of the support provided, associated challenges and opportunities to improve from the lived experiences of providers. Following semi-structured interviews with 12 participants, findings confirm results presented in earlier literature and provides new insights. Each participant had exposure to numerous SMEs, in some instances hundreds, at a regional or national level due to their roles at their respective organisations. The inherent knowledge gained from this exposure results in each participant's experience representing the cumulative experience of several SMEs as opposed to a singular view of one. We conclude that there is a vast amount of cyber security related content aimed at SMEs and our findings reveal providers are playing an assistive role in the understanding, education and implementation of cyber security defences. Despite significant efforts being made, cyber hygiene amongst SMEs remains low and they are unlikely to proactively reach out for support. Additionally, SMEs have low knowledge levels and are hampered in their efforts due to comprehension, capability, attitudes, and resources whilst providers face numerous internal and external challenges when delivering this support. Insights from data reveal several opportunities for improvement can be realised through the creation of security focused communities that can provide support, collaboration and learning.

1. Introduction

Small- and Medium-Sized Enterprises (SMEs) constitute a large portion of organisations within any given country and collectively contribute significantly to their respective economies. As an example, in the UK, 99.9% of the 5.6 million businesses are classified as SMEs, employing three-fifths of the workforce and generating approximately half of the turnover in the private sector (FSB, 2023). Therefore, the cyber security of SMEs and their resilience to attacks becomes an important aspect to safeguard in order to secure the overall resilience of the economy that is moving towards digitalisation. Additionally, the Covid-19 pandemic accelerated organisations' reliance on Information Technology (IT) to conduct their day-to-day operations (Kergroach and Bianchini, 2021). Despite this uptake in the use of technologies by SMEs, larger businesses are more likely to have a formal cyber security strategy in place and be able to identify attacks than smaller ones (DSIT, 2024). This government cyber security breaches survey revealed that only 28% of micro-sized

organisations have formal documentation or cyber security policies in place and 27% included cyber security aspects as part of their business continuity plans. Among those businesses that identify a breach or an attack 44% end up being victims to some sort of cybercrime. Despite these statistics, the survey unveiled only 12% of businesses are reportedly aware of government initiatives to defend against attacks, such as the Cyber Essentials scheme. Awareness levels appear to be proportional to the business size with a high contrast in awareness levels amongst medium (43%) and large businesses (59%) when compared to 12% of overall businesses (DSIT, 2024).

Perhaps due to this low awareness levels amongst organisations that fall towards the smaller end of the 'SME' scale, there continues to be a stubbornly slow uptake amongst businesses in implementing robust passive cyber defences, such as those found in Cyber Essentials scheme, to improve their baseline cyber security measures. Simultaneously, falling victim to a cyber-attack can have significant impact on businesses that extends from internal information systems to business continuity, economic and financial reputation, legal ramifications and on their associated supply-chains (Pirounias and Patsakis, 2014; Tetteh, 2024; Chaudhary et al., 2023). However, cyber security research in the context of SMEs remains an understudied topic area (Alahmari and Duncan, 2020). In addition to the challenges posed in identifying a breach, a majority of research studies focus on specific typology of attacks with few studies examining impacts that go beyond the technical and operational aspects (Fernandez De Arroyabe and Fernandez De Arroyabe, 2023).

Furthermore, there is a lack of research that examines the delivery of cyber security advice from the perspective of those that provide it. In an effort to examine the journey SMEs undertake to secure themselves, this research study does so through the lens of advice providers. Providers of security advice are often not solely responsible for generating and/or promoting established advice from credible sources, but they often bridge the gap between advice being published and its adoption. This bridging results in providers having a nuanced understanding of the security journey of SMEs through their exposure to them, which can shed light on SMEs' motivations to become cyber secure, challenges they encounter, aspects that work well and areas that can benefit from improvement in the future.

The subsequent sections of this article are structured as follows. Section 2 provides an overview of relevant work that discusses cyber security in the context of SMEs. Section 3 provides the research methods utilised in this study. Section 4 presents thematic findings from qualitative interviews about the cyber security related support needs of SMEs from the lived experiences of providers. Section 5 holds a discussion of the findings in the context of literature and highlights aspects that can benefit from improvements in the future. Finally, Section 6 concludes this article by summarising key findings, limitations of the research study and suggests avenues for future research.

2. Background

A vast amount of cyber security literature and guidance is available to SMEs which is varied in its coverage of topics, completeness and clarity (Khan et al., 2024). Overwhelming amount of information alone can cause confusion amongst the SME audience and can hamper their efforts to improve their security as the advice can be contradictory and confusing (Renaud and Weir, 2016). A potential way of improving SMEs' engagement with cyber security is through improving the accessibility and usability of information being provided to them (Wilson and McDonald, 2024; Chaudhary et al., 2023).

A study by Redmiles et al. (2020) examined the quality of security and privacy advice being provided online, examining various aspects for comprehensibility, actionability, and efficacy. Participants, comprised of users and professionals, evaluated unique pieces of security advice to evaluate the quality of content. Findings showed that users were left to independently choose, prioritise, and action advice that subsequently creates a range of

challenges in the implementation of security defences. Whilst users' status of employment was not an aspect explicitly covered in this research study, it can reflect similar real-world settings to those classified as sole traders, micro, and small enterprises within the larger SME umbrella. In addition to the gap in knowledge about how they comprehend or action the information available to them, and whilst SMEs are recognised to be targets of attacks, there is a lack of information about attempted attacks encountered by SMEs or their associated impact (Arroyabe et al., 2024).

Arroyabe et al. (2024) also discuss the lack of standardisation for cyber security measures for businesses from an administrative or governmental level and noted that this area can benefit from benchmarked compliance measures that are similar to ISO27000 and Cyber Essentials. Gundu and Flowerday (2013) highlight the same point, namely for UK government to introduce a merit system to showcase the cyber security hygiene of businesses. They argue for a similar stance to be adopted as when dealing with the control of infectious diseases and replicating the success enjoyed by the Food Hygiene Rating Scheme that depicts food hygiene of businesses on a five-point scale.

A review by Chidukwani et al. (2022) discovered that advice is narrowly focused on identify and protect components within the NIST framework and neglects the remaining elements i.e. detect, respond and recover. Furthermore, their findings revealed that SMEs are challenged by their lack of financial and human resources (including technical expertise), issues with regulatory compliance, and a general lack of knowledge of how to protect themselves against an attack. Low levels of knowledge amongst SMEs can extend to not knowing which assets to protect (Bada and Nurse, 2019; Osborn and Simpson, 2018; Paulsen, 2016). This can potentially account for the low-readiness levels amongst SMEs for their cyber security and resilience.

The attitudes of SMEs towards cyber security can also be correlated to their cyber security posture in literature. For instance, two independent studies in the US and South African regions have shown that SMEs underestimate their cyber security risk (Rohn et al., 2016; Kabanda et al., 2018). Another study by Thompson (2023) showed a direct correlation between cyber security risk and the lack of resources, lack of awareness, and the use of outdated technology in small businesses. These variables are believed to improve if businesses prioritise cyber security as part of their daily operations. Risk appetite (Henson and Garfield, 2016; Mmango and Gundu, 2020) and the perception of impact in smaller businesses (Gundu and Flowerday, 2013; Tetteh, 2024) have also been noted as variables that can play part in the cyber security posture of SMEs. Bhattacharya (2015) argued that cyber security activities are not believed to be a valuable contribution to the core business in the same way as sales or revenue and are thus likely to be neglected. This point is furthered by Wong et al. (2022) stating that it results in SMEs falling short in their cyber security concerns and preparedness for attacks. A survey of attitudes towards cyber security amongst UK SMEs showed that they did not believe that they would be victims to a cyber-attack (Wilson et al., 2023). Furthermore, Chidukwani et al. (2022) state that SMEs' attitudes towards cyber security practices can relax over time as there are no tangible benefits that emerge from their effort and investment.

However, there is limited research that examines the journey or lived experiences of SMEs when they decide to secure themselves including their efforts to become resilient following an incident or a breach. In order to improve cyber security amongst SMEs, it becomes important to understand how they make decisions, the sources they use, the circumstances under which they take action, any challenges they face, and the effectiveness of the support being provided to them – all factors that influence and effect the outcomes of their security and resilience. Additionally, providers are well positioned to share insights garnered from their experiences when supporting SMEs through this journey as they often bridge the gap between advice being published and its adoption. In this context, providers are uniquely

positioned in their exposure and intrinsically have rich experiences that can offer valuable insights that can benefit current understandings.

3. Research methods

A qualitative research study was designed to explore employee experiences at organisations that provide cyber security guidance to SMEs. A qualitative approach was chosen as it provides an opportunity to develop an in-depth understanding of the cyber security related support needs of SMEs by learning from the lived experiences of those that provide it. The study focused on three areas. Firstly, to understand the various types of cyber security support offered by providers in their natural contexts (Malterud, 2001). Secondly, to understand the cyber security topics for which support is sought and the circumstances under which support is requested by SMEs. And thirdly, to explore the extent to which the support offered by providers was believed to be effective, including aspects such as the skills required to provide cyber security support to SMEs, challenges encountered by providers and any lessons learnt. Questions shown in Table 1 were utilised to explore these aims through semi-structured interviews. This technique offered a nuanced understanding of participants lived experiences when discussing sensitive issues inherent to this topic (Adams, 2015).

No.	Category	Question
1	Scene setting	What types of support does your organisation offer to support cyber security for SMEs?
2	Scene setting	How often do SMEs approach you for support?
3	SME support needs	Are there any noticeable trends in terms of the types of organisations that seek support?
4	SME support needs	What issues do SMEs typically seek support about?
5	SME support needs	How would you describe the typical cyber security knowledge of those seeking support?
6 (a)	Effectiveness of support	Do have a sense of whether SMEs typically understand the support they're provided?
6 (b)	Effectiveness of support	Do you have a sense of whether SMEs are in a position to do what is needed?
6 (c)	Effectiveness of support	Are there any limiting factors?
7	Effectiveness of support	Do you have a sense of whether the support typically leads to a successful outcome?
8	Effectiveness of support	Do you know if the support you provide is effective and how?
9	Effectiveness of support	What do you think are the skills required to provide effective cyber security support to SMEs?
10	Effectiveness of support	When providing this support, which aspects do you think work well?

11	Effectiveness of support	What are some of the challenges you face when providing this support?
12	Effectiveness of support	In your opinion based on your experiences, how do you think things be improved?

Table 1. Semi-structured interview questions to explore the organisational experiences of providers that offer SMEs cyber security guidance.

It is worth noting that whilst the participants offer valuable insights for support needs of SMEs in the domain of cyber security, these views are constructed in the organisational contexts, sector of operation and larger societal constructs and might differ from other stakeholders for the types of support requested and its delivery (Willig, 2008).

Following ethical approval, twelve participants were recruited to represent various provider perspectives. A sample size of twelve was deemed suitable to answer the research questions due to the appropriateness of data offered by participants in their roles (O'reilly and Parker, 2013), due to the suitability of the organisations i.e. organisations that provided cyber security support to SMEs or had a dedicated arm which offered it, and due to interviews reaching data saturation (Bekele and Ago, 2022). It is important to note that whilst the sample size is arguably small, each participant had appropriate knowledge required for this study i.e. the ability to comment on their organisational experience in relation to providing cyber security guidance and support to SMEs. Additionally, participants' respective organisations had exposure to numerous SMEs, with some having exposure to hundreds as part of their roles at a regional or national level. This exposure subsequently represents intrinsic knowledge that providers have garnered from experiences with a magnitude of SMEs. Furthermore, data saturation can occur within this sample size as it can be reflective of the similar experiences and challenges being faced in the UK when supporting SMEs with their cyber security at a regional and national level. Similar sample sizes have been used in other research studies when applying qualitative techniques whereby participants were deemed to have appropriate experience at relevant organisations. For instance, a study by Waelchli and Walter (2025) utilised eight participants for semi-structured interviews who were recruited through the professional network of the first author. This was deemed suitable as participants were selected due to having appropriate knowledge on a range of cyber security topics necessary to investigate ways to reduce human susceptibility to social engineering. In another study by van der Kleij et al. (2022) a sample size of ten participants from three organisations was appropriate due to the relevant experience offered by the participants. Subsequently, findings offered insights to develop techniques to support management's decision making when encountering cyber threats or incidents. Another study that examined measures to prevent knowledge leakage in organisations (Ahmad et al., 2014) utilised eleven participants. This sample size was also deemed appropriate due to the nature of organisations and the knowledge offered by participants which is intrinsic to their experience in their roles. Other studies also support the use of smaller sample sizes where participants belong to specific organisations and are believed to have appropriate knowledge needed to shed light on the topic being investigated (van de Weijer et al., 2024 with n=11; Zanke et al., 2024 with n=10).

Participant designations are shown in Table 2 below. Participants were recruited though snowball sampling that involved advertising the call to this study through the professional network of the authors. Selection of participants was based on their ability to provide relevant data based on their roles at suitable organisations. Organisations were deemed suitable if they acted in a supporting capacity to SMEs for matters pertaining to their cyber security either exclusively or had a dedicated team performing this function within the larger organisation. As a result, participating organisations were based across the UK, belonged to

the private, public and non-profit sectors with their own strategic objectives guiding the nature of their support. Thus, representing the broader provider ecosystem in the UK.

To initiate or improve their cyber security defences, SMEs can have contact with one or multiple providers that are best suited to their needs. This can result in SMEs being advised or seeking advice from a range of sources. For instance, they might seek advice from their insurance provider who currently supplies them with other forms of insurance and/or, seek guidance from their internet provider or a security vendor that provides related services such as equipment or IT services and/or, approach a not-for-profit organisation they are affiliated with or a government body to request support. The nature of organisations has been generalised to ensure anonymity of participants and this study's sample shows representation from various organisations who act as providers, which have been categorised as follows:

- Named body in the security/tech/business space i.e. they provide information and assistance related to security, technologies and operation of businesses and/or consumer rights
- Government department or body
- Insurance providers i.e. companies that provide cyber security insurance
- Security vendor i.e. organisations that provide security education or defensive software to SMEs, and
- Dedicated body in the SME space - i.e. refers to dedicated, not-for-profit organisations that work to further national strategic objectives

One participant offered cyber security support to SMEs in their capacity as a 'client' to their supply-chain. Thus, they provided advice to numerous UK based SMEs which was deemed suitable for the purposes of this research. For this reason, the participant's *Category of Provider* is listed as 'Other' in Table 2.

SMEs were not included as part of this study as they would only be able to offer experiences from a singular or individual entity perspective, whilst noting that it would contain various pathways or avenues 'within' their journey to become cyber resilient. However, providers were deemed more suitable as their interactions, and subsequent experience, contains a magnitude of SME journeys and subsequent pathways they choose to adopt. Thus, speaking to providers was deemed to contain richer data and oversight than that which could be garnered from interviewing individual SMEs.

No.	Category of Provider	Role
P1	Named body in the security/tech/business space	Chief Executive Officer
P2	Named body in the security/tech/business space	Deputy Head of Insurance
P3	Other	Senior Manager
P4	Government body	Head of Department
P5	Insurance provider	Product Leader
P6	Security vendor (software, education)	Chief Solutions Architect
P7	Security vendor (software, education)	Director
P8	Security vendor (software, education)	Associate
P9	Dedicated body in the SME space	Managing Director
P10	Dedicated body in the SME space	Chief Executive Officer
P11	Dedicated body in the SME space	Head of Cyber Security
P12	Security vendor (software, education)	Cyber Security Consultant

Table 2. Providers and participant designations

Participants were not offered any compensation for sharing their organisational experiences and were provided with associated materials to share the motivations of this study prior to recruitment. Participants were also provided the opportunity to ask any questions prior to commencing interviews, after interviews and reminded of their rights before concluding each session.

Data was collected between February and March 2024. Interviews were conducted virtually via Microsoft Teams in a one-to-one setting with the lead author, generating approximately 7 hours of dialogue. These discussions were audio and video recorded and transcribed verbatim from the digital recordings. All participants were anonymised, and identifiable traits removed from the transcripts as part of the 'data processing' stage. Transcripts were independently checked for accuracy and effective anonymity by the other authors before digital recordings were permanently deleted. Participants are referred to as P1, P2 and so on and any identifiable features such as names or frequent words used in language were redacted (for example "[[name of person]]") to safeguard anonymity. To demonstrate the significance of findings whilst safeguarding anonymity of participants, terms such as 'few', 'several', 'many' and 'all' were considered (Braun and Clarke, 2021). For the purposes of openness and transparency, the number of participants evidencing themes is shared as part of the findings section where values should not be interpreted in the same fashion as those in a quantitative study to ensure the integrity of results.

Following the data processing stage, transcripts were uploaded to Lumivero-NVivo software for coding (Lumivero, 2024). Template analysis was utilised (King, 2012) whereby a template containing broad parent themes along with nested child themes was used to code data (top-down approach). With the application of grounded theory approach to the data (Glaser and Strauss, 2017; Muller and Kogan, 2012) the initial template was updated with new parent and child themes as they emerged (bottom-up approach). Template analysis technique was suitable as it provided researchers with flexibility, time efficiency compared to other approaches (such as IPA, Spiers and Smith, 2019), is not infused with a particular methodological or theoretical position and allows flexibility within the coding structure. Codes were then compared against each other from within and across transcripts known as constant comparison method (Hoda et. al, 2010) until data saturation was reached before commencing analysis. Codes and respective data were checked independently by other authors for accuracy, discussed and re-coded as appropriate. Appendix A provides the codebook with parent and child themes that emerged from the data.

4. Results

The following section presents findings about the cyber security related support needs of SMEs from the lived experiences of providers. In doing so we explored the nature of support provided, cyber security topics that are frequently discussed and the circumstances in which SMEs seek support. Provider perceptions about successful outcomes were also examined as well as the skills required to provide support, associated challenges providers face with SMEs, and lessons learnt when engaging in support related activities. Quotes from interview data are shared to exemplify themes that emerged from the template analysis.

4.1 Provider landscape

This section discusses the types of support available to SMEs and the skills needed by providers to effectively deliver guidance.

4.1.1 Types of support

Ten participants shared that they offered very specific services that demarcated their involvement, responsibilities, and positioning from other providers in the cyber security ecosystem: "*We've been doing some work with the cyber resilience centres, so we try and*

engage locally where we can, through activities like that" [P2] "*Our main support is one of education and awareness, and where we can, for instance through third parties, offering practical information and tips*" [P1] and, "*That's not what we do. There are plenty of other products which are excellent that do that*" [P8]. With this demarcation providers collaborated with, or referred SMEs to, other organisations that were better suited to their circumstantial needs: "*We do push them towards support organisations. We have a very good relationship with Action Fraud, the local Rokus across [[region name]], and so we always do put them in contact with these law organisations. And say 'Just make sure, before you do anything, you get their advice and guidance*" [P6].

All providers discussed offering an array of services to SMEs, including promoting governmental advice, tools, training and services offered by the National Cyber Security Centre (NCSC), forming communication channels with local police and other crime reporting bodies (for example police cyber alarm), and sign posting resources, services and cyber security qualifications from 3rd party vendors. For instance: *"For Cyber Essentials, we're obviously always trying to promote that and push people in that direction"* [P9] and, "*It's that focus on SMEs to bring [them] some of these products, anything from vulnerability scanning through to end point protection*" [P7]. Additionally, providers mentioned offering their own services which included technical solutions and assessments, training, awareness and education, consultancy and evaluating organisational processes and policies, and managing governance, risk and compliance: "*We typically offer risk assessments [and] risk management services. So, it's more focused on the 'governance, risk and compliance' when it comes to SMEs. Stemming from that, depending on what we find when we do a gap analysis or anything situated to their industry or their risk levels, then we can mitigate based on the back of that [analysis]*" P12. Providers also offered proactive or reactive incident response and offered solutions from other providers and services that are affordable and suited to SME needs. This is reflected in a conversation with P4, "*We directly provide incident response training and generic cybersecurity training… We also provide funding for cyber essentials to selected vulnerable sectors*".

All providers shared the various ways in which SMEs were able to benefit from their support. For instance, face-to-face activities which included in-person visits to local businesses and exhibits, offering hands-on activities and trainings, participating in interactive sessions that involve questions and answers, and offering remote/virtual resources in written or video formats. Providers also leveraged other ways of furthering their reach through social media channels, websites, blogs, emails, phone calls, and through 3rd parties such as collaborations (with MSPs or member bodies), recruiters and brokers.

The providers were engaging with a wide demographic in terms of types of SMEs, and all discussed serving businesses ranging from sole traders, micro-organisations to medium-sized organisations: "*We do consume a lot of small businesses and bigger ones too through the pipeline [supply chain] … we do sometimes work with smaller companies, start-ups and so on*" [P3]. Providers' demographics were also varied in their language, income, number of employees and in their nature of business for instance, industry of operations and physical and hybrid operations: "*Who we work with, they typically vary across locations [and] across industries*" [P12]. Additionally, eleven providers engaged with SMEs that were locally based: "*About 95% are micro businesses, something around about 78% are sole trader. It's a really interesting and challenging demographic for us to support … [[Region name]] is a is obviously a very diverse [[area]]. I think it's got [[a lot of]] different languages that are spoken*" [P10] and, "*Focus [for us] is small and medium enterprises in [[region name]]*" [P4] and, "*We focus a great deal on SMEs… we try and engage locally where we can and encourage brokers who are [[a part of the organisation]] to engage locally as well*" [P2].

4.1.2 Skills

The skills needed to deliver effective support to a diverse audience was repeatedly highlighted. For instance, five participants mentioned adjusting their support to suit the technical needs of the SME and building good rapport with them. Rapport building skills included being able to provide guided walk-throughs and the SME having trust and confidence in the provider.

Seven providers shared the need to have technical cyber security skills, which could be in varying degrees from beginner to advanced level: "*Sometimes the advice can be super simple like access controls, encryption, logging, monitoring, alerting, that kind of stuff. That's pretty basic. If you're getting really deep into that [cybersecurity] space, then you might need someone who's got some really specialised knowledge*" [P3] and, "*We do obviously have people who have those technical skills… even on the technical side, we need to make sure that the behaviours within the SME or, the 'client', will match the technical side. There's no point in having an antivirus if they disengage it, switch it off or don't update it*" [P8]. Their prior experience was viewed as a vital element that added the ability to know best practices and promptly identify the state of systems in order to deliver effective support: "*You need huge, huge levels of experience to deliver effective guidance and support*" [P9] and "*I wouldn't expect a CISO to be able to be a pen-tester for instance, they're completely different skill sets. But I think identifying what's where and who needs to do it, is very key*" [P7].

The need for non-technical or 'soft skills' was also noted. Five providers shared that empathy was important as it can help providers understand SMEs circumstances and feelings: "*That ability to be able to address more vulnerable customers, to have that empathy, and that compassion for your customers. And not just treat it as you're just doing your job*" [P5] and, "*For myself and [[my senior partners]] it's less technical stuff now… It's probably we've more become counsellors in these situations*' [P6] and, "*Making sure that they [SMEs] understand that you have the best intentions and also understanding that they probably have good intentions too*" [P3] and, "*It's no good, from a cyber security vendor perspective, trying to peddle something onto them (SMEs) that just doesn't fit their context. So, empathy is a big one*" [P12]. This understanding allowed providers to develop a closer relationship with SMEs and motivate them to make recommended changes.

Five providers discussed the importance of having the ability to understand how businesses operate as part of soft skills: "*The real skills I think are… and this is the really difficult part, is people understand how a business operates*" [P10] and, "*We do a lot of context gathering at the beginning to try and make sure we understand the client as much as we can so that when we come to recommend stuff it's feasible*" [P12]. This included being able to understand business operations and financial limitations but also the overarching impact of an incident on the business that might involve legal obligations such as reporting data breaches.

Three providers emphasised that good listening skills allow them to understand SMEs needs, reservations and determine favourable outcomes pre and post incidents: "*Being able to listen to the clients' issues and what the concerns are there*" [P8] and, "*Listening [as a skill] it really opens up the conversation when you just let them speak and see where things go… So, trying to understand different pain points really, because everybody has their own opinion*" [P12]. The ability to communicate was also identified as an important skill by ten participants. This encompassed being able to translate technical knowledge into a format that can be understood by laypersons, as well as having the ability to communicate with various designations within organisations who might possess different experience levels and backgrounds: "*There's so many different messaging and campaigns and a lot of our job is to try and demystify it [cybersecurity] and to try to speak English [layperson terms] and I'm not overly technical to these (SME) organisations*" [P4] and, "*Once you've lost your*

audience, then they've turned off. You might as well just be speaking French to them. So, talk in a language that people will understand" [P11] and, "*Without that communication skill I'd be dead in the water, either if I couldn't speak to the techie guys, or I couldn't speak to the board. You've got to be able to do both*" [P7]. Additionally, it was important for communications to be simple, transparent, tailored, and frequent: "*The ability to not over complicate things, to make it easy to understand, to articulate it easier*" [P5].

Six providers discussed the ability to locate suitable resources and provide practical guidance: "*I can at least give them a steer on how, even if that's just linking off to some docs that are on like an Amazon Web page or something. It's like, here's how to do this thing*" [P3] and, "*Being very clear about what the response should be, what they can do and signposting very clearly*" [P1]. Guidance included aspects such as directing to appropriate supporting bodies and understanding the application of guidance documents that entail governance, risk and compliance.

As a summary, the following points highlight key findings from this section:

- Whilst providers distinctly position themselves for the support they provide, there is an array of services on offer
- These services can be provided for proactive (improving cyber security prior to a breach or an incident) or reactive (following an incident or a breach to improve resilience) measures. Support is provided in a number of formats
- Providers engage with a wide demographic of SMEs and tend to focus their efforts more regionally
- In order to deliver support, providers need a range of skills that include not just technical but also a number of soft skills such as, empathy, listening, communication etc., that they find are essential for effective delivery to support SMEs

4.2 Provider Experiences

This section discusses provider experiences which includes how success is measured, aspects that work well, hurdles that providers encounter, and opportunities to improve cyber security support for SMEs in the future.

4.2.1 Aspects that work well

'Connecting' with SMEs and in-person interactions are two main aspects that work well for providers. The wider discussions around this theme included eight participants sharing techniques used by their organisations. These included provider efforts to cater to different forms of learning (such as including visual learners) and offering relatable examples: "*Q&A sessions, breakout sessions and hands-on things, they work really well for different types of learners and visual learners. Some people just absorb stuff like a sponge, some people need to do things to do the learning. So, I think you need to understand your audience*" [P9]. They also shared that demystifying technical language and including foreign languages spoken amongst their audience perform well in their efforts to provide support: "*The engagement we got from that was so much better. This isn't just about the technical language being put into simple English, it's also about translating it into the language that these people are more comfortable in engaging with*" [P10]. As part of connecting with SMEs, providers shared that conducting training sessions, identifying appropriate support for them (such as guidance documents or experts), and simplifying technical knowledge and guidance are also positive aspects: "*During our training that people go, 'Oh, I didn't realise that that was a form of scam' or 'Now I get it. I won't do that again'. That's more qualitative data where you can observe a culture change, which could take up to nine months in an organisation*" [P11]. Using existing support materials (e.g. from NCSC) and creating new support materials tailored to their audience were well received. Finally,

developing long-term relationships with SMEs proved to be another element that has a favourable impact when providing support: "*It's making sure we touch base with them. And of course, we do a lot of webinars and white papers but also, things coming out from NCSC. We make sure that SME's account manager's feeding them information throughout the year. So, they just don't come back every year when they need a renewal*" [P6].

Additionally, three providers believed that in-person activities were more impactful than other forms of interaction, resulting in better rapport and offering personalised or hands-on training where needed. In-person activities were also seen to be more appropriate for effective delivery of cyber security knowledge which is the case for other statutory health and safety training: "*If you do online cyber security training, you're trying to teach them weaknesses and exploits on the same platform that are likely to be scammed on. You don't deliver First Aid training online, do you, realistically? You've got to do CPR in person*" [P11], and "*My view is that's the only way of making sustainable change in behaviour, is to physically have feet on the ground*" [P10].

4.2.2 Success and its measures

All providers believed that their support typically leads to a successful outcome. 'Success' is viewed differently between providers as they deliver various types of support. However, seven providers did not have a complete picture to enable them to measure the effectiveness of the support they provide: "*If they're taking car transactions [and] if you're accepting credit cards… they may go straight to [[e-commerce provider name]], as opposed to come to us… So we wouldn't see that (side of the conversation) necessarily*' [P1]. While providers are knowledgeable of the extent of their support, they are uncertain about how much of their advice is implemented by SMEs and to what extent. Thus, providers find it difficult to categorically measure the effectiveness of support provided by them: "*Because we're signposting information and we're giving guidance, you don't necessarily see the end result*" [P2] and, "*The feedback that we do get, and again it's skewed, isn't it? Because the people who won't tell you that you've a good job are the ones who didn't think you've done a good job and, the ones who have not engaged or don't think they have, tend not to bother*" [P9].

Six providers also shared measuring the overarching effectiveness of their support from the absence of a cyber security incident. The absence of a cyber security incident or event can indirectly showcase their contribution to a safer environment: "*If an SME gets a breach, then it's not very effective, I'd say*" [P7] and, "*If you have Cyber Essentials accreditation, you are less likely to, now nothing's fool proof [but], you're less likely to be subjected to a cyber-attack and obviously you're increasing the resilience of the organisation*" [P4]. These providers highlighted the predicament of measuring cyber security success, which is more pronounced in pre-emptive efforts: "*The difficulty with crime prevention is that, how do you prove that a person has not become a victim of a crime by the activity you've done?*" [P9] and, "*No one has yet suffered a cyber-attack or a ransomware attack who's got our product. But that's what it's designed to do, to stop that [threat]*" [P8].

Possibly to overcome the theoretical challenge of measuring security success in the absence of an event, eleven providers discussed applying a mixture of qualitative and quantitative techniques to measure the effectiveness of their support. These showcase the diverse ways in which different aspects are being measured by providers:

- Qualitative techniques included soliciting feedback in written and verbal formats and receiving testimonials. Feedback measurements include positive sentiments and negative experiences, such as SMEs reporting challenges they encountered from the support provided and raising their concerns. Providers also measure their success indirectly i.e. by helping SMEs to implement the NCSC's Cyber Essentials (CE) standard

- Quantitative approaches included surveys, click-rates on public facing materials and sign-ups to services and tools such as CE, trainings, accreditation vouchers or the use of incident helplines. Additionally, providers measured baseline improvement on indicators such as technical vulnerabilities, employee awareness levels and phishing susceptibility levels prior to and post providing support. Where relevant, providers measure various metrics to indicate the recovery of SMEs following an incident

4.2.3 Challenges

Providers reported a range of challenges they face when providing support i.e. compensating for messaging done in technical terms, limited internal resources, efforts to self-promote, achieving set targets and adjusting to demand fluctuations, and overcoming mistrust associated to the cyber security domain. These provider challenges are distinct from aspects discussed in the next section pertaining to SMEs as these are 'internal' to providers (as opposed to being external factors which would limit their ability to control outcomes).

More widely, information about cyber security is still being provided in technical terms and forms a language barrier with audiences according to eight providers: "*In the guidance we give, we dedicate about two, three or four pages to what these terminologies mean*" [P2] and, "*Just saying, 'Right, you need to do a pen test. Oh, that's going to cost about £6-10,000. See you later, there's my report'. That clearly doesn't work*" [P7]. The language and messaging used for cyber security results in SMEs being victimised, confused, overwhelmed, or inattentive to communications: "We make a conscious effort in [[region name]] to be more positive about cyber… *A lot of the messaging is very negative so, 'if you don't do this, this is what will happen' and the business reaction to that is to switch off*" [P10]. Providers thus face the challenge of providing information to compensate for these language and messaging barriers: "*We've given SMEs something, but we need to be able to manage that message better*" [P5].

Eight providers discussed the challenges that emerge from a lack of internal resources. Limitations included lack of human resources, not having enough individual or organisational capacity, and managing a finite amount of funds: "*The problem is we can't go and help everybody because we just don't have the capacity to be able to do it*" [P5] and, "*If I could have a team that was double the size, I could go out and have someone out there every single day delivering those messaging*" [P4] and, "*To be constantly engaged in a dialogue I think would be desirable. Not necessarily easy, because both sides could [/would need to] have resources to do that. But that would be nice*" [P2]. Providers are also challenged by the need to stay abreast of the field and engage with training at a personal or organisational level. At an organisational level they face challenges to promote themselves, deliver on set targets and adapt to the varying needs in demand: "*From our perspective, because we're small [business] ourselves, typically, everybody's using different tools, different systems, et cetera, et cetera. And these might have not been things [/tools] that we've dealt with before. So, it's a first-time experience for us. So, there is a bit of a learning curve on our end*" [P12] and, "*We ourselves are an SME, we do worry whether we are going to meet our own targets in providing a good service. So, making sure that we have the capacity to deliver*" [P8].

Additionally, three providers faced the challenge of overcoming the general mistrust of SMEs when approaching providers and disclosing cyber incidents. Mistrust is also exercised by SMEs when validating cyber security expertise claimed by individuals, believing systems are secure or that the advice is for their own benefit: "*There's a general level of mistrust, a bit like a used-car salesman. It's unfair, but it still exists within the SME market about mistrusting the cyber security industry as a whole*" [P9].

4.2.4 Opportunities to improve

Further efforts can be made to include wider audiences within the cyber security domain, an aspect captured in ten provider discussions. More specifically discussions included making efforts to involve more SMEs and engage those that do not proactively approach providers for support. Engaging alienated SMEs was believed to have more impact as they would be arguably the most vulnerable having not received any prior support or advice: "*There are SMEs that haven't been victim of the loss or need some extra education, it's those people that are probably falling short*" [P5] and, "*When we are really into our subject… we forget that we haven't taken everybody else from that layperson bench with us*" [P8] and "*If you get [SMEs] on board early, yes, they're not perfect, but you can help tailor a bit more to what you're needing*" [P3].

As part of the inclusion theme, providers also believed that real-world examples should be utilised to include alienated audiences which allows SMEs to relate to the information being shared: "*Really bringing that message home, bringing real-life examples so we're not preaching but rather bring the audience with you*" [P4] and, "*It comes back to also using businesses as examples and making sure that the advertising will connect them (campaigners) with small business owners in the right way*" [P1]. Further efforts are required to educate SMEs about cyber security. For instance, through providing trainings that can include awareness training and the use of technical tool and solutions, teaching (i.e. learning courses) and propagating a no-blame culture.

Seven providers also shared that it is important for SMEs to actively engage with cyber security. Active engagement was believed to enhance communication between providers and SMEs whereby SMEs can better understand cyber security, openly request help, ask questions and provide feedback: "*We want to encourage people to collaborate and participate to improve their resilience. To be constantly engaged in a dialogue I think would be desirable*" [P2]. Active engagement would support frequent interactions, create learning opportunities and collaborations between peer-to-peer groups such as within SMEs and between providers: "*Security communities, I think that is fantastic. I see it as almost like self-help groups… it's just a place where everyone can get on a level pegging*" [P7] and, "*It's hard to find people in our position, our size from a cyber security perspective, who are offering services that are also cost effective for SMEs… Somehow bridging the partnership aspects and being more collaborative with others is something I wish was a bit better*" [P12]. Active engagement was also believed to help encourage SMEs to implement proactive measures and bring all parties on the same page when interacting with cyber security topics.

Several aspects were highlighted by eight providers that can benefit from improvements at national and overarching policy level. This included better collaboration and cross-cutting communications between governmental departments. Businesses should be financially incentivised to improve their cyber hygiene or consider cyber security aspects at the time of their inception: "*Maybe there needs to be more financial incentives for businesses to get that help*" [P2]. Tools and platforms should have robust default security settings and enhanced security features should not be at an additional cost to consumers: "*Security measures should be like a mandatory opt-in*" [P11]. Vendors should be transparent about their prices and the applicability of their solutions for SMEs. Current efforts by government were believed to be in a positive direction however, existing areas can be further improved: "*You've got [[government department names]], all these different departments and they're all working to try and improve cybersecurity… But in different ways, at different rates, and often working cross-purposes to each other and briefing against each other, sometimes not even realising that they're doing it*" [P9]. Another area for improvement is adapting current content to better suit SME contexts, increased efforts to raise awareness, standardising terminology, and connecting networks together: "*I've seen the current government campaign about making individuals aware of fraud with their bank accounts,*

fraud with their e-mail. Maybe that campaign should look at small businesses and small business owners being the target" [P1].

Six providers emphasised the importance of distinguishing between the sizes of organisations that are classified under the broad term of 'SME' in order to understand their needs, awareness levels and ways of work: "*There's a vast difference between small or affiliated, and medium [sized organisations]*" [P8]. This understanding can aid in tailoring communications, guidance, and services that are fit-for-purpose: "*Content needs to be appropriate for the target audience. And what I mean by that is, a one-size-fits-all approach isn't going to work*" [P10].

Finally, four providers considered that the cyber security sector should be better regulated, and organisations should be compliant to minimum cyber security standards: "*There needs to be a minimum standard for every organization that is operating online to have something in place*" [P9] and, "*They will only have Cyber Essentials if there's a business requirement for them to do it. At the moment, cyber is still seen as a 'should do' [and] 'not a must*" [P11]. With the noted success of Cyber Essentials in defending against successful cyber-attacks, providers highlighted the need for organisations to be compliant with CE or a similar service. Providers believed that at a governmental level, CE adoption should be encouraged or mandated, it should be made more affordable and be better suited to smaller organisations – all of which were believed to reduce barriers to its adoption.

As a summary, the following points highlight key findings from this section:

- Tailoring support, using laypersons language, developing long-term relationships and in-person interactions were all believed to be aspects that work well for providers.
- How success is measured varies between providers as it is devised by the organisation and can involve qualitative, quantitative or mixed techniques
- Providers themselves face a range of challenges in their efforts to deliver effective support to SMEs such as, translating technical knowledge, limited or lack of internal resources, improving their organisational visibility, achieving agreed targets, and adjusting to fluctuating demands
- More can be done to include additional SMEs or a wider audience within the cyber security domain. This inclusion is believed to be most needed by SMEs who have been completely disengaged or alienated in the past or those that do not proactively reach out for support. Inclusion can be improved through the use of real-world examples, education and training, utilisation of technical tools, instilling a no-blame culture, and improving communications
- At a national level and overarching policy level in the UK, various aspects can be enhanced such as: introducing financial incentives or baseline cyber security requirements for businesses, end-user technologies to be secure-by-design, transparency from security vendors about pricing and applicability of solutions to SMEs, better collaborations and communications between departments, adapting current content to better suit SMEs, raising awareness, standardising terminology and connecting wider networks together. Further improvements can be made to reflect the nuances found in the broad term of 'SMEs' and measures such as Cyber Essentials should be suitable, affordable and encouraged for their adoption

4.3 Challenges with SMEs

This third and final section shares findings that related to challenges faced by SMEs. This included themes that reflected trends, the frequency of contact between providers and SMEs, circumstances under which support is sought, knowledge levels, and SMEs ability to act effectively.

4.3.1 Trends

Providers shared trends that they had observed when providing advice and support. Six highlighted low readiness levels amongst SMEs to identify or protect against cyber-attacks. Additionally, three cited basic levels of cyber hygiene being implemented by SMEs: "*The trends that we're seeing, it's the really basic stuff that they just haven't got at all*" [P10]

Another trend identified by five providers was the difficulty in exclusively targeting or engaging specific sectors and domains versus casting a widespread net to get audiences. Five participants noted a trend of increased engagement from specific sectors like education, public sectors, healthcare, and charities. Furthermore, three participants believed that the demand for cyber security was also being driven by increased importance on governance, risk and compliance with SMEs being told to improve by regulatory bodies or clients: "*From a small business perspective, a lot of the trend has been governance and insurance driven*" [P6].

Seven participants noted increasing attention being paid to smaller organisations at a national level by government: "*We're starting to see that emphasis go more towards that SME route*" [P5]. One participant further believed that increased exposure through online operations would subsequently increase the demand for support in the future.

4.3.2 Contact Frequency

There was a polarising response in terms of how frequently SMEs made contact, with most providers stating a more intermittent pattern. More specifically, eight providers shared that they experienced a 'low level' (i.e. less than once a week or an unknown level) of proactive contact from SMEs reaching out to them for support whilst four participants indicated contact at least once a day. Nine participants shared that the interactions providers did have were due to them (or their collaborators) proactively engaging with SMEs and the contact frequency is thus dependent on their efforts of engagement: "*It's being very proactive, and outreach is a key part of that. As opposed to sitting back and waiting for enquiries to come in*" [P10].

4.3.3 Circumstances when requesting support

The general impression from eleven provider discussions is that SMEs approach them for support reactively. Contact most commonly occurs following a concern for exposure or an incident which compromised SME's systems or data. The circumstances for approaching providers following an incident meant SMEs had little knowledge of the steps they needed to take going forward at the time initial contact was made. This results in SMEs finding themselves in unfortunate circumstances before seeking advice or support "*Quite often, certainly with SMEs, it's off the back of an incident… they realise sometimes when it's too late*" [P7]. Thus, providers are initially faced with providing support to contain the impact and subsequently prevent the SME from being a victim in the future.

Providers also cited other reasons for SMEs approaching them. For instance, if the SME saw an awareness campaign that heightened their concerns over the integrity of their technologies (cited by three participants), concerns to improve their baseline hygiene when requested by a client (cited by three participants) or to request training (cited by two participants).

4.3.4 Knowledge levels

Eleven providers discussed the low levels of cyber security knowledge that exists amongst SMEs: "*It's been quite alarming to see how poor their cyber security posture is. It's the really basic stuff that we're just not seeing at all*" [P10]. Thus, there is a lack of

understanding about fundamental measures normally form the first line of passive defences such as, strong passwords, updates, data back-ups and multifactor authentication.

Providers also highlighted a range of aspects more generally. For instance, SMEs were believed to lack knowledge about how guidance from government departments (such as NCSC) was applicable to their organisations. There was also a lack of knowledge about the roles and responsibilities relating to cyber security, including those associated with specific cyber security positions, those relating to their Managed Service Provider (MSP) and those concerning all employees. SMEs reportedly did not have the knowledge to make informed decisions i.e. when adopting technologies and identifying symptoms of an attack: "*Recognising symptoms and bad behaviour of a computer is probably out of reach of your average small business owner. They won't even know about things called 'end of life' and supported devices*" [P11]. Additionally, it was mentioned that SMEs have little knowledge about how to improve their cyber security and operated with a lack of in-house IT skills. This resulted in SMEs attempting to secure themselves with limited knowledge and thus with limited success: "*If you're running a shop, the chances are you don't have an IT department. You haven't got that expertise in your employee base, to necessarily to pick up on the issues you as a business need to know*" [P1].

Low levels of cyber security knowledge also meant that SMEs are limited in their ability to safeguard themselves from attacks or be resilient to them. Greater knowledge was apparent amongst those approaching providers proactively. However, this was potentially due to other factors such as, having previously been a victim to a cyber-attack or if the business operated in a security centric domain: "*For those who come to us for help, knowledge is higher because they've already gone over that hurdle or speed bump in the road such as an incident*" [P9].

4.3.5 Ability and Willingness to Act

Three aspects emerged when discussing SMEs' ability to act on advice they are provided that can subsequently affect their cyber security and resilience: comprehension, capability, and their attitudes and limitations.

According to nine providers, SMEs' comprehension of guidance was reportedly low at the time of their first interaction. Five providers stated that this improved with subsequent contact: "*Sometimes the guys [business] will look at you and he's got the whites in his eyes and he's like, 'What? What are you on about? I've got no idea what vulnerability scanning is, like [what]?'. So, what we have tried to do was to make that journey simpler*" [P6] and, "*I would say SMEs understand and that's because we have a lot of communication with them*" [P12]. A range of actions emerged as part of discussions around providers efforts to improve SMEs' comprehension. For instance, translating technical knowledge to layperson audiences, assisting the guidance process in incremental stages, highlighting aspects that can increase vulnerabilities, and generally educating their audiences: "*We're seeing where we have to spend more time with them, spend more attention with them, to walk through that process with them, it is more towards that micro side of it. You'd see where you're really having to help and walk through that process more than anything*" [P5] and, "*We quite often see there is no process in place. So, we help them [SMEs] introduce processes which we try and compare to First Aid training and Fire Alarm training… We've produced 'cyber posters' which replicate the same sort of content*" [P11].

All providers felt that SMEs' capabilities to improve their posture was linked to a range of factors. Seven emphasised the adversities faced by smaller organisations: "*You can do a lot with technical tools but not if you don't have the People and the Process. My experience is that a lot of the smaller businesses, they have no one doing IT or networking*" [P6] and, "*If you've only got £100,000 company turnover… I'm pretty sure they (organisation) are not going to get anybody working for them for £4-6,000 per year, right? So, they're not going*

to have that in-house expertise until they grow to a certain level" [P5]. These factors included a lack of resources such as not having time (seven participants), monetary funds (eleven participants) and access to technical expertise (eight participants): "*Access to capital, access to funding, access to the skills that SMEs need. Security engineers are very expensive so getting one dedicated can be a lot, especially if you're a small organisation. For businesses that in regions that are not specialised it can be hard. If you live in the middle of nowhere, it's probably a lot harder*" [P3] and, "*Budget is definitely a huge problem. And the price the 3rd party vendor quoted me, I was thinking, 'there's no way they (SME) are going to pay that' because it's just way too much out of their scope. And that's a big problem*" [P12].

Five providers mentioned smaller organisations lack capacity more generally in their human resourcing, as well as individual capacity when people are performing multiple functions: "*You've got to be the stock taker, the accountant, the HR department, the tax department, all in one. And you've got to then think about technical issues like cybercrime*" [P1] and, "*A lot of the SMEs I speak to at the moment are in what's called survival mode. Since COVID, they've really been all hands [[on deck]]. So whereas [in the past] a Manager or Director used to be able to stand back and manage their business, they are now pretty much on the shop floor as one of the workers, doing the due and [also] being the Manager*" [P11].

Various factors emerged when discussing SMEs ability to act competently in the context of cyber security. All providers believed that SMEs are largely unaware of cyber security, and associated risks to cyber security are an unknown domain for them. This means that SMEs do not know the support they require, avenues to receive it, or if they have increased risk exposures: "*Because they don't know where to go and they don't know what help they need*" [P10] and, "*I don't think small businesses really understand what these controls actually do and what they mean for the business. And then at that point they've accepted the risk*" [P6] and, "*The vast majority of businesses that we talked have got no idea. They're working with insecure websites that 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].

Ten providers felt that SMEs do not prioritise cyber security activities in the same way as their other responsibilities, especially those that are critical to their operation: "*I think it's the understanding of the issue like not prioritizing cyber security. Spending £20,000 to go to a trade event seems like a priority over spending £20,000 and having a secure network. So, they might have the money, but they want to spend it in other ways*" [P9] and, "*It's probably not seen as a big priority because they can't quantify the risk or for them there are other things (like) the day job is far more important*" [P10] and, "*They [SMEs] see cyber security as supportive to their business, but maybe they don't feel it's fundamental*" [P2].

It was also believed by nine providers that SMEs held negative or apathetic attitudes towards cyber security. This predisposition does not allow them to see the value or benefit in the help they are provided. Resultingly, initiatives or efforts made by providers to improve cyber security are undersubscribed or providers encounter an attitude whereby SMEs appear to be disengaged or not care about this topic area in their daily operations. For instance, a quote from a discussion with P8, "*It may be seen as a 'big business issue' and not a small business problem… Smaller organisations will allocate funds to this problem unless they have a problem with it*" and, "*Until something happens on their website or social media that directly impacts them or somebody very close to them, it [cyber security] is not an issue. But I can understand, somebody who has no technical knowledge and they just want to run their small little business. And there are resources available which they can run, for either no cost or very little cost, but is there the willingness? I don't know*"

[P6] and, "*The average small business owner also doesn't really have the aptitude for that [cyber security] either. And they don't care… Small businesses don't think it's really for them*" [P11].

Nine providers painted a picture of proactively initiating contact and following up with the SMEs to overcome apathetic attitudes. This includes making regular contact to share knowledge or enquire about the status of SMEs cyber security: "*We reach out regularly, and we revisit these organizations two or three times, sometimes four times in a year, just to see how they're getting on and whether need extra help*" [P10] and, "*They come to us, they do something and then probably half of them forget about it. The other half are pretty good. We reach out to them quarterly, they go, 'Thank you. It was useful. I've read through it, or I skimmed through it'. The other half just ignore it*" [P6].

SME often believe that they are unlikely to be victims of a cyber-attack. Ten providers discussed how SMEs do not prefer disclosing if they had been a victim in the past, engaging in conversations about their cyber security nor knowing about potential vulnerabilities that might exist within their organisation: "There's still that mindset in small businesses where, '*It happened to that guy. I'm too small'. There's still that thing 'I am too small'. They [SMEs] will contact us and then they'll say, 'You know what, okay, just talk to my IT person or company. Sort it out. I don't really want to know*" [P6] and, "*That 'plausible deniability'. They feel comfortable not knowing than knowing there is a problem*" [P9]. SMEs may also believe that the responsibility for cyber security lies with someone else, which can include inaccurately believing that MSPs are responsible as part of their IT service packages: "*There's always been this reliance upon organisations, particularly in the SMEs space, where they would say, 'Okay, that [cyber incident] is never going to happen to us. And if it does happen to us, then we've got insurance to cover us'*" [P5] and, "*SMEs seem to think it's someone else's problem to solve. So, the individuals seem to think that cyber is not something they themselves need to worry about or take responsibility for*" [P8].

Furthermore, five providers suggested that attitudes made it challenging for SMEs to understand the impact of a cyber security incident. Since actions occur in the digital landscape SMEs struggle with the real-world impact that can emerge if they are compromised: "*When you talk about crime, they tend to focus on physical or verbal crime because that's more tangible than something that you can't see, like cybercrime. You can't see it until its happened*" [P1]. This also shows a disconnect that SMEs experience in trying to connect cyber actions and digital assets to real-world settings: "*If something happens to your car you can visually see it. And then when that car's been repaired, you can visually see that it. Whereas with cyber, you don't always see it*" [P5] and, "*We all know what a fire and a flood does, but an awful lot of people don't know what a cyber-attack does*" [P2].

SMEs attitudes included the misconception that improving their cyber security posture will be financially costly (mentioned by five providers). The fear from this misconception adversely affected their attitudes that restricted SMEs from improving their posture: "*There is a perception that cyber security just costs lots of money. So, there's no point even doing a small amount*" [P8] and, "*They have a fear that cyber is going to suddenly cost them huge sums of money. We try and take away some of those common fears straight away*" [P10].

Four providers indicated that where SMEs approached them for support, the interaction was linked to revenue generation and/or retention: "*We're seeing a lot more demand, because SMEs are getting the scary supplier assessments through, so they're potentially losing business or not winning business that they should be winning*" [P7]. This attitude meant that becoming cyber secure or complying with industry standards such as ISO, was a segue to their financial growth rather than a journey in itself: "*Cyber is still seen as a 'should do' and 'not a must do'*" [P11] and, "*From a small business perspective (it's) 'Oh,*

I've had an incident' or, 'My supplier which is [[a large retailer name]] is now asking me to do these security related stuff, and I don't really know what they mean' … it's a tick-box sometimes" [P6] and, "*They are required to maybe get some compliance to win work on their end. So, they might require Cyber Essentials for example, or someone told them to do ISO 27,001. Then they'll reach out to us*" [P12].

As a summary, the following points highlight key findings from this section:

- There is a low-readiness level amongst SMEs to identify and protect against attacks with difficulties arising from targeting support to specific sectors. Demand is driven by compliance requirements, with smaller organisations being the focus at a national level
- SMEs infrequently approach providers for support with providers proactively initiating contact with SMEs. Contact most commonly occurs by an SME if they have been a victim to an attack or suspect they might be easy targets. Providers subsequently support SMEs in their resilience
- Providers experience low levels of cyber security knowledge amongst SMEs. This included a lack of knowledge about fundamental security measures, applicability of guidance, roles and responsibilities with cyber security, and technology security. Additionally, SMEs are not aware of ways to improve their security posture or be resilient to attacks
- Comprehension, capability and attitudes adversely affects SMEs' ability and willingness to act when improving their security and resilience. Comprehension was improved through sustained interactions and efforts made by providers. Capability to improve is dependent on a range of factors such as a lack of resources such as time, money and access to technical expertise, with smaller organisations facing magnified challenges due to their size. Being unaware about cyber security, competing priorities, holding negative or apathetic attitudes, and shifting responsibility are some of the aspects that limit SMEs ability and willingness to act effectively in the context of cyber security. Additionally, they struggle to understand the impact of a breach or an incident, believe that security measures are costly and improvements to their posture are being driven by revenue generation or retention

5. Discussion

Findings from this study support earlier literature evidence that there is a vast amount of cyber security information targeting the SME audience (Khan et al., 2024; Renaud and Weir, 2016). From the twelve participating organisations a range of services they offer were discussed. These were presented in various forms and formats that could be pre or post cyber incidents. Potentially in the face of this landscape, providers appear to distinctly position themselves and showed signs of collaborating with others when needed.

Redmiles et al. (2020) discuss how SME users are left to their own devices to select, prioritise and implement advice best suited to their needs. It was also noted by Renaud and Weir (2016) that the overwhelming amount of information can cause confusion and hamper SME efforts in becoming secure. Providers shared their role of assisting SMEs in their effort to improve their security and resilience through various initiatives. These include providing activities and interactive sessions as well as trying to reach disengaged audiences. As part of these assistive outreach activities, providers noted serving a diverse demographic with a regionally focused approach. These findings reflect providers filling in the vacuum that existed between the advice being published and its implementation and aiding in reducing confusion amongst SMEs when trying to become cyber resilient. To deliver this function effectively providers shared an array of skills that are needed. These range from technical to soft skills such as communication, trust building, relationship building, and being able to locate and assist with implementing appropriate guidance.

When noting trends that emerged from provider experiences, there was an emphasis on governance, risk and compliance (GRC). This emphasis was driven by regulatory bodies or clients with an increased importance on securing smaller sized organisations. Despite the focus of guidance arguably being on identify and protect elements within the NIST framework (Chidukwani et al., 2022), our findings showed that providers are still encountering very low baseline cyber hygiene amongst SMEs. Encouragement from regulatory bodies for GRC and the focus on smaller organisations are both potential drivers that can see an improvement in SMEs' security and resilience to cyber-attacks in the future.

Findings also showed the frequency of interactions between the providers and SMEs is primarily dependent on the efforts made by providers. This means that SMEs are less likely to proactively reach out to providers with cyber security related queries. Additionally, when this contact does occur proactively from an SME it is often due to an accidental exposure or a cyber security incident.

The lack of knowledge amongst SMEs poses a challenge for providers. Arroyabe et al. (2024) point out the lack of information about attacks on SMEs and its subsequent impact. Findings discussed in Section 3 highlighted a lack of knowledge amongst SMEs about adoption of technologies and identification of attacks. This lack of ability to identify attacks, i.e. understanding symptoms of an attack or protect against vulnerabilities emerging from unsupported technologies, can provide a potential explanation for under documented experience of SMEs being targeted. It also supports the findings reported by Chidukwani (2022) whereby SMEs are challenged by the lack of technical expertise. Furthermore, they do not have the know-how to protect themselves against an attack. Data from this study gave supporting evidence as SMEs were not able to identify appropriate guidance that would be best suited to their needs or circumstances. Since SMEs have limited technical knowledge about technologies, for e.g. supported technologies versus unsupported devices, by virtue this can indicate and provide evidence to support earlier literature about SMEs not knowing which assets to protect (Bada and Nurse, 2019; Osborn and Simpson, 2018; Paulsen, 2016). Additionally, findings show SMEs lack knowledge about roles and responsibilities for cyber security within their ecosystem.

SMEs are restricted in their ability to act effectively due to comprehension of content, abilities, attitudes and due to other limitations. To improve comprehension providers are delivering tailored support to improve understanding within this domain. Providers shared that smaller organisations face increased adversities due to their size. For instance, in their lack of resources (time, money, human resources), and access to technical expertise, all of which is further magnified by regional disparities. These demands on resources, which are amplified for smaller organisations discussed in Section 4.3.5, can in turn affect SMEs' capability in improving their cyber security posture. These findings support research presented earlier (Chidukwani et al., 2022; Tetteh, 2024) where these limitations act as a barrier for SMEs when improving their security. Additionally, risk appetite was another factor noted in the findings that stems from SMEs' lack of knowledge and inhibits their ability to act competently in the context of cyber security. This risk appetite is a variable that can affect the overall security posture of the organisation (Henson and Garfield, 2016; Mmango and Gundu, 2020).

With the lack of resources available to SMEs discussed above, overall lack of knowledge, and the utilisation of outdated technology are all variables that directly correlate with cyber security risks faced by an organisation. Thompson (2023) argues that this risk can be reduced when organisations prioritise cyber security as part of their daily operations. Findings from this study showed organisations fail to prioritise cyber security in the same way they would other critical activities, such as sales and revenue. Furthermore, SMEs did not see the value in the help provided resulting in undersubscribed services and are disengaged from cyber security in their daily operations. This supports the argument made

by Bhattacharya (2015) that organisations do not view cyber security activities as a valuable contribution in the backdrop of business-critical operations (Wong et al., 2022) which can result in cyber security being neglected.

There is a relaxed attitude amongst SMEs towards cyber security. Providers compensate for this by initiating engagement and periodically sharing knowledge or requesting updates. This supports findings by Chidukwani et. al (2022) whereby the lack of tangible benefits from efforts and investment in cyber security is believed to result in disengagement which effects the overall cyber security posture of the organisation.

Studies by Rohn et al. (2016) and Kabanda et al. (2018) showed SMEs underestimate risks connected to cyber security. Findings presented by Wilson et al. (2023) highlighted that SMEs did not believe that they could be victim to a cyber-attack. Discussions with providers evidenced SMEs believing that they are an unlikely casualty of an attack. SMEs also did not prefer to disclose if they had been victims in the past or being made aware of their potential vulnerabilities. SMEs also externalise the responsibility of cyber security to others in their ecosystem. Furthermore, SMEs struggle to associate digital actions to similar actions in real-world settings. Perception of actions and impact can result in increased risky behaviours online and, as argued by Gundu and Flowerday (2013) and Tetteh (2024), can intertie with the overall security posture of SMEs. Another perception noted in the data was SMEs believing that securing their organisation or improving their posture would be costly. When providers were approached by SMEs it is driven by retaining or generating revenue. Thus, security measures are perceived to be a segue to financial security or growth by SMEs rather than an act in and of itself. Overall, the above attitudes can indirectly increase SMEs' risk exposures and misinform their opinions and understandings which can subsequently affect their cyber security and subsequently their resilience.

When discussing aspects that work well, responses reflected the importance and success from inclusion of diverse audiences. Providers were able to include diverse SMEs through catering to various forms of learning, tailoring content to suit needs and increasing the accessibility of technical guidance documents. Accessibility was improved through translating guidance to layperson experiences and into foreign languages. This supports findings from Wilson and McDonald (2024) which suggests increasing the accessibility of cyber security content to improve engagement from SMEs. It is important to note here, from findings reported later on in Section 4.2.3, these efforts are in response to challenges that are inherent to existing guidance documents. For instance, information continues to be published in technical terms, language used further victimises SMEs, causes confusion or is overwhelming –ultimately leading to their disengagement from this domain. This provides evidence in line with findings from a study by Chaudhary et al. (2023) presented earlier with the challenge of improving the usability and delivery methods of cyber security content. Additionally, findings reveal that establishing long-term relationships and in-person engagements were aspects that work well for providers when improving SMEs' cyber security.

As discussed above, Arroyabe et al. (2024) note the lack of information about attacks on SMEs. When discussing measures of success, findings show that despite providers' relatively close relationship with SMEs, they did not have a complete picture of subsequent actions SMEs undertook post their interaction. Additionally, findings highlight the paradox of measuring safety success in the absence of an event. Consequently, providers deploy a range of qualitative, quantitative or mixed techniques to measure their success. These measures are devised by the provider organisations and are varied, suggesting a lack of standardisation in this domain to measure success or the effectiveness of support efforts.

Whilst findings evidence providers bridging the gap between published advice and its adoption, responses highlight the difficulty providers face by their own limited organisational resources. These challenges are similar to those faced by SMEs themselves

such as, limited internal resources, improving their organisational visibility, adjusting to fluctuations in demand, staying abreast of the field, engaging in trainings, and overcoming distrust present in the cyber security domain.

Findings reflect efforts made at a governmental or administrative level within the UK are in the right direction but can benefit from further improvement. Firstly, collaboration and cross-cutting communications between departments can be enhanced. From the time of their inception, businesses can be encouraged to consider cyber security related aspects in the same way as other requirements which document plans critical to their operation. Existing organisations can be incentivised to improve their cyber hygiene. Digital tools and platforms should have robust default security configurations promoting 'secure by design' principles and additional security features should not be at a further cost to clients. Cyber security vendors can be required to be transparent about their pricing and applicability of solutions to the SME demographic. Existing guidance issued by government can also be enhanced to better suit SME contexts with increased efforts for its awareness. Terminology can be standardised and established networks can benefit from being better connected. Previous research also highlights the need for intervention at a governmental level to establish similar compliance standards seen implemented for ISO or food hygiene ratings for businesses (Arroyabe et al., 2024; Gundu and Flowerday, 2013). Findings from this research have furthered this point and shown a call from providers for government to regulate the cyber security sector, and introduce minimum standards in business operations. Additionally, there should be compliance to Cyber Essentials and compliance to such standards should be better suited to SME contexts and be affordable.

Findings reveal a number of opportunities to aid efforts in improving SMEs' cyber security and resilience as reported in Section 4.2.4. These opportunities further the case for the creation of virtual security communities that provide cyber security support through bridging the gap between providers and organisations across regions. For instance, groups can be utilised to onboard SME audiences who have not yet had the chance to address their cyber security needs and are identified to be at the highest risk of exposure and vulnerability. This can be achieved in several ways such as organic growth (word-of-mouth sign-ups) or targeted advertisements. A community centric platform can also offer experience-sharing opportunities for organisations through posts to stimulate active engagement. Sharing experiences can allow organisations to communicate their lived experiences with the wider community. This sharing would offer examples that resonate closely with the lived experiences and challenges faced by others, instil peer-to-peer learnings, contribute to improved security cultures, and further efforts to improve knowledge and education. Additionally, communities can be engineered to pronounce the nuances that exist within the broader SME umbrella and allow regionally or industry sector focused approaches to improve the relevance of information on offer. Communities of support can also contribute effectively towards establishing open communications that destigmatise the cyber security domain, facilitate channels to request help, ask questions, and provide feedback on sought support. Finally, communities that involve providers can create opportunities to establish two-way communication streams and collaborations whereby providers can impart credible information and answer queries that SMEs might otherwise find difficult to ask.

6. Conclusions

This study has explored aspects of SMEs' cyber security journeys, in terms of how they decide to become cyber secure, improve their resilience and the associated efforts they make to improve these aspects. Since there is limited research on this topic and about the ways in which SMEs engage with cyber security, data was gathered from the lived experiences of organisations providing cyber security advice and services. Providers are well positioned to shed light on this topic area as they bridge the gap between the advice being published and its adoption. By virtue of doing so, they are in a unique position to have a nuanced

understanding of adoption practices in the SME sector and tacit knowledge about advice's application in real-world settings.

Findings confirmed that there is a vast amount of information targeted at the SME audience for cyber security which is presented in various formats and positioned for pre or post incident contexts. In a saturated landscape, providers position themselves and their services distinctly from others in the ecosystems and show early signs of cross collaboration where clients are referred to others if they're deemed to be better suited to SME's needs at the time of contact. Findings highlight the assistive role providers are playing in driving the adoption of cyber security measures and reduce confusion. While they serve a diverse demographic, efforts are regionally focused and require an array of technical and soft skills to effectively deliver services. Governance, risk and compliance (GRC) is noted to be a driver for improving cyber security through encouragement from providers or clients. However, the baseline cyber hygiene amongst SMEs remains low and SMEs are unlikely to proactively reach out for support.

Findings show SMEs knowledge levels are low for their understanding of the field, technologies and technical expertise. Low knowledge levels hamper their ability to identify attacks. This in turn can provide rationale for the under documented experience of SMEs being targeted that is reported in literature. The lack of technical expertise hampers SMEs' ability to protect themselves against attacks and would increase their attack surfaces and thus, their susceptibility to an attack. In addition, the lack of technical knowledge and expertise provides evidence for SMEs not being able to identify and effectively protect important assets nor demarcate the roles and responsibilities for cyber security within their ecosystem.

At a national level, communications between departments can be enhanced, revisions can be made to legislation to improve baseline cyber security hygiene within organisations and security features to be mandated for digital solutions and services. The sector can also benefit from transparency in costings and applicability of solutions being offered by vendors, and guidance can be more suited to contexts by recognising the nuances that exist within the broad term of 'SMEs'. Whilst efforts are being made at a national level to increase SMEs' cyber security and subsequent resilience, findings have highlighted additional opportunities for improvements. These include connecting providers and SMEs (especially those that are at high risk of becoming a victim), fostering collaboration and promoting peer-to-peer learnings. A potential way of realising these insights is through the creation of security communities that incorporate these features in its design.

Although a diverse set of organisations participated in this research, snowball sampling can limit the variety of participants and in turn the generalisability of the findings. Views shared by participants are informed by their organisational contexts, sector of operation and larger societal norms so the generalisability of findings to other countries would be limited. Additionally, views shared by participants might differ from other stakeholders within their organisation due to their designations, nature of work and daily level of involvement in the delivery of support.

Further research will address a more in-depth examination of the journeys or lived experiences of providers and SMEs, in order to understand paths taken by SMEs to become cyber secure and resilient. These research efforts can aid in developing an understanding of such contexts to inform the design and delivery of support communities that can benefit from peer-to-peer collaborations, destigmatise this topic area and aid in including alienated SMEs.

Acknowledgements

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 (RISCS).

Corresponding author: Neeshe Khan; neeshe.khan1@nottingham.ac.uk

Appendix A: Codebook

Parent and child themes in the data across the 12 interview files.

Parent Theme	Child Theme
1. Provider Landscape	
	Types of Support
	Skills
2. Challenges with SMEs	
	Trends
	Contact Frequency
	Circumstances
	Knowledge
	Ability to Act
3. Provider Experiences	
	Aspects that work well
	Success and its measures
	Challenges
	Opportunities to improve

References

Adams, W. C. (2015). Conducting semi-structured interviews. Handbook of practical program evaluation, 492-505. https://doi.org/10.1002/9781119171386.ch19

Ahmad, A., Bosua, R., & Scheepers, R. (2014). Protecting organizational competitive advantage: A knowledge leakage perspective. Computers & Security, 42, 27-39. https://doi.org/10.1016/j.cose.2014.01.001

Alahmari, A., & Duncan, B. (2020, June). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In 2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA) (pp. 1-5). IEEE. https://doi.org/10.1109/CyberSA49311.2020.9139638

Arroyabe, M. F., Arranz, C. F., De Arroyabe, I. F., & de Arroyabe, J. C. F. (2024). Exploring the economic role of cybersecurity in SMEs: A case study of the UK. *Technology in Society*, *78*, 102670. https://doi.org/10.1016/j.techsoc.2024.102670

Bada, M., & Nurse, J. R. (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

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

Bhattacharya, D. (2015, September). Evolution of cybersecurity issues in small businesses. In *Proceedings of the 4th Annual ACM Conference on Research in Information Technology* (pp. 11-11). https://doi.org/10.1145/2808062.2808063

Braun, V., & Clarke, V. (2021). Thematic analysis: a practical guide. Sage Publications

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2023). A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. Computer Science Review, 50, 100592. https://doi.org/10.1016/j.cosrev.2023.100592

Chidukwani, A., Zander, S., & Koutsakis, P. (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

DSIT. (2024, April 09). Cybersecurity breaches survey 2024. GOV.UK. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024

Fernandez De Arroyabe, I., & Fernandez de Arroyabe, J. C. (2023). The severity and effects of Cyber-breaches in SMEs: a machine learning approach. *Enterprise Information Systems*, *17*(3), 1942997. https://doi.org/10.1080/17517575.2021.1942997

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 14/10/2024. (2023)

Glaser, B., & Strauss, A. (2017). *Discovery of grounded theory: Strategies for qualitative research*. Routledge. https://doi.org/10.4324/9780203793206

Gundu, T., & Flowerday, S. V. (2013). Ignorance to awareness: Towards an information security awareness process. *SAIEE Africa Research Journal*, *104*(2), 69-79. https://doi.org/10.23919/SAIEE.2013.8531867

Henson, R., & Garfield, J. (2016). What attitude changes are needed to cause smes to take a strategic approach to information security?. Athens Journal of Business and Economics, 2(3), 303-318. https://doi.org/10.30958/ajbe.2-3-5

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

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, *28*(3), 269-282. https://doi.org/10.1080/10919392.2018.1484598

Kergroach, S., & Bianchini, M. M. (2021). *The digital transformation of SMEs*. OECD Publishing.

Khan, N., Furnell, S., Bada, M., Nurse, J. R., & Rand, M. (2024). Assessing Cyber Security Support for Small and Medium-Sized Enterprises. Retrieved from https://nottingham-repository.worktribe.com/output/901361

King, N. (2012). Doing template analysis. Qualitative organizational research: Core methods and current challenges, 426, 426-450. Sage Publications Ltd.

Lumivero (2024) NVivo (Version 12.7.0) www.lumivero.com

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

Mmango, N., & Gundu, T. (2023, November). Cyber Resilience in the Entrepreneurial Environment: A Framework for Enhancing Cybersecurity Awareness in SMEs. In 2023 International Conference on Electrical, Computer and Energy Technologies (ICECET) (pp. 1-6). IEEE. https://doi.org/10.1109/ICECET58911.2023.10389226

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.

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

Osborn, E., & Simpson, A. (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

Paulsen, C. (2016). Cybersecuring small businesses. *Computer*, *49*(8), 92-97. https://doi.org/10.1109/MC.2016.223

Pirounias, S., Mermigas, D., & Patsakis, C. (2014). The relation between information security events and firm market value, empirical evidence on recent disclosures: An extension of the GLZ study. *Journal of Information Security and Applications*, *19*(4-5), 257-271. https://doi.org/10.1016/j.jisa.2014.07.001

Redmiles, E. M., Warford, N., Jayanti, A., Koneru, A., Kross, S., Morales, M., ... & Mazurek, M. L. (2020). A comprehensive quality evaluation of security and privacy advice on the web. In *29th USENIX Security Symposium (USENIX Security 20)* (pp. 89-108).

Renaud, K., & Weir, G. R. (2016, August). Cybersecurity and the unbearability of uncertainty. In *2016 Cybersecurity and Cyberforensics Conference (CCC)* (pp. 137-143). IEEE. https://doi.org/10.1109/CCC.2016.29

Rohn, E., Sabari, G., & Leshem, G. (2016). Explaining small business InfoSec posture using social theories. *Information & Computer Security*, *24*(5), 534-556. https://doi.org/10.1108/ICS-09-2015-0041

Spiers, J., & Smith, J. A. (2019). Interpretative phenomenological analysis. SAGE Publications Ltd.

Tetteh, A. K. (2024). Cybersecurity needs for SMEs. Issues in Information Systems, 25(1). https://doi.org/10.48009/1_iis_2024_120

Thompson, J. (2023). Factors Influencing Cybersecurity Risk Among Minority-Owned Small Businesses. *Reviews of Contemporary Business Analytics*, *6*(1), 29-42. Retrieved from https://researchberg.com/index.php/rcba/article/view/114

van der Kleij, R., Schraagen, J. M., Cadet, B., & Young, H. (2022). Developing decision support for cybersecurity threat and incident managers. *Computers & Security*, *113*, 102535. https://doi.org/10.1016/j.cose.2021.102535

van de Weijer, S., Leukfeldt, R., & Moneva, A. (2024). Cybercrime during the COVID-19 pandemic: Prevalence, nature and impact of cybercrime for citizens and SME owners in the Netherlands. *Computers & Security*, *139*, 103693. https://doi.org/10.1016/j.cose.2023.103693

Waelchli, S., & Walter, Y. (2025). Reducing the risk of social engineering attacks using SOAR measures in a real world environment: A case study. *Computers & Security*, *148*, 104137. https://doi.org/10.1016/j.cose.2024.104137

Willig, C. (2008). Introducing qualitative research in psychology: Adventures in theory and method account.

Wilson, M., & McDonald, S. (2024). One size does not fit all: exploring the cybersecurity perspectives and engagement preferences of UK-Based small businesses. *Information Security Journal: A Global Perspective*, 1-35. https://doi.org/10.1080/19393555.2024.2357310

Wilson, M., McDonald, S., Button, D., & McGarry, K. (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

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

Zanke, A., Weber, T., Dornheim, P., & Engel, M. (2024). Assessing information security culture: A mixed-methods approach to navigating challenges in international corporate IT departments. *Computers & Security*, 103938. https://doi.org/10.1016/j.cose.2024.103938

CRediT Statement:

Neeshe Khan: Conceptualization, Formal analysis, Investigation, Methodology, Writing – original draft, Writing – review & editing. **Steven Furnell:** Conceptualization, Methodology, Supervision, Validation, Resources, Project administration, Writing – review & editing. **Maria Bada:** Conceptualization; **Matthew Rand:** Writing – review & editing; **Jason R.C. Nurse:** Conceptualization, Methodology, Writing – review & editing.

Declaration of competing interest:

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Vitae (Biographical Sketch)

Neeshe Khan is a Research Fellow in Cyber Security for Cyber Security Communities of Support (CyCOS) at the University of Nottingham. As part of this role, Dr Khan investigates the SMEs' journey to become cyber secure and the design of security communities to support

these endeavours. Her research interests include human factors in cyber security within organisational contexts through the lens of risk & safety engineering approaches. Her PhD from the University of Nottingham investigated factors that influence unintentional insider threat to identify and limit accidental cyber security breaches. Dr Khan has collaborated with higher education institutes globally, governmental bodies, private firms and worked on national level cyber security challenges concerning various aspects of the human element. She champions diversity in STEM and has given interviews and made TV appearances to encourage females and BAME in the science domain.

Steven Furnell is Professor of Cyber Security in the School of Computer Science at the University of Nottingham. His research interests include security management and culture, usability of security and privacy, and technologies for user authentication and intrusion detection. He has authored over 390 papers in refereed international journals and conference proceedings, as well as various books, book chapters, and industry reports. Steve is the UK representative to Technical Committee 11 (security and privacy) within the International Federation for Information Processing, and a board member of the Chartered Institute of Information Security, and a member of the Steering Group for the Cyber Security Body of Knowledge (CyBOK) and the Careers and Learning Working Group within the UK Cyber Security Council. Steve is also the Principal Investigator on the CyCOS project, looking at enhancing cyber security support for small organisations.

Maria Bada is a Senior Lecturer in Cyberpsychology at Queen Mary University in London. Her research focuses on the human aspects of cybercrime and cybersecurity, such as profiling online offenders, studying their psychologies and pathways towards online deviance as well as the ways to combat cybercrime through tools and capacity building. She is a member of the National Risk Assessment (NRA) Behavioural Science Expert Group in the UK, working on the social and psychological impact of cyber-attacks on members of the public. She has a background in cyberpsychology, and she is a member of the British Psychological Society and the National Counselling Society.

Matthew Rand is a Postdoctoral Research Assistant in the School of Biological and Behavioural Sciences at Queen Mary University in London. Matt has a background in psychology, and his research interests include cyber security behaviour change, cyber security culture, the measurement of cyber security behaviours and risk perception within cyber security. Matt has previously worked as a Behavioural Scientist in cyber security teams within large multinationals, with the core aim of reducing cyber security risk to the organisation through the behaviour of their employees. Matt started his career within an SME and is a keen advocate of reducing cyber risk in small and medium sized organisations. He also has a PhD from the University of Sheffield in the area of Behaviour Change.

Jason R. C. Nurse is a Reader in Cyber Security in the Institute of Cyber Security for Society (iCSS) & School of Computing at the University of Kent, UK. He also holds the roles of Visiting Fellow in Defence & Security at Cranfield University, UK and Associate Fellow at the Royal United Services Institute for Defence and Security Studies (RUSI). He received his PhD from the University of Warwick, UK. His research interests include cyber resilience, security risk management, security culture, cyber insurance, corporate communications and cyber security, and insider threat. Jason was selected as a Rising Star for his research into cybersecurity, as a part of the UK's Engineering and Physical Sciences Research Council's Recognising Inspirational Scientists and Engineers (RISE) awards campaign. Dr Nurse has published over 100 peer-reviewed articles in internationally recognised security journals and conferences, and he is a professional member of the British Computing Society.