Designing Cyber Security Communities of Support to improve SME cyber hygiene and resilience

Neeshe Khan[1][0000-0003-3962-7305], Ram Herkanaidu[1][0000-0003-2294-0899], Steven Furnell[1][0000-0003-0984-7542], Jason R.C. Nurse[2][0000-0003-4118-1680], Maria Bada[3][0000-0003-0741-5199], and Matthew Rand[3] [0009-0009-2446-0259]

[1] School of Computer Science, University of Nottingham, Nottingham, UK
[2] School of Computing, University of Kent, Canterbury, UK
[3] School of Biological and Behavioural Sciences, Queen Mary University of London, London, UK
neeshe.khan1@nottingham.ac.uk

Abstract. Small-to-Medium-sized Enterprises (SMEs) represent the vast majority of businesses in the UK and many other countries. At the same time, however, SMEs can often lack preparedness in relation to cyber security. This becomes problematic for SMEs in their own right, as well as in the context of supply-chains for larger organisations. Despite the availability of information and resources many SMEs are challenged by a lack of understanding and skills to help address questions and enact advice. Based upon ongoing research into the support available to SMEs, this paper proposes the concept of Cyber Security Communities of Support. The discussion presents the principles of the communities, as well as various practical considerations to be accounted for in operationalizing the approach (including the provision of an online Support Broker platform as an enabler for community dialogue). Finally, attention is given towards the planning for a series of pilot communities, from which it is intended that the findings will help to provide the basis for an ongoing and replicable model of support.

Keywords: Cyber security, SMEs, Small Businesses, Communities, Cyber Security Support, networks, collaborative learning, shared expertise

1 Introduction

It is widely recognized that Small-to-Medium-sized Enterprises (SMEs) can find themselves challenged by cyber security. In the UK, the most recent Cyber Security Breaches Survey suggests that half of small businesses have experienced a cyber security breach or attack in the last 12 months, while at the same time showing that such organisations are much less likely to have relevant controls in place than their larger counterparts [1]. At the same time, SMEs represent a significant provider of employment and account for a significant proportion of the economic value in many countries [2]. Again, using the UK as a specific example, the 5.5 million SMEs collectively account for 99.8% of businesses and three fifths of employment (16.6

million people), and half of the turnover (£2.8 trillion) in the private sector [3]. As such, they collectively represent a critical national asset that merits appropriate protection.

The need to support SME engagement with cyber security is well-known, and there are various routes through which support can be sought, including online guidance and via third-party service providers. However, what is less clear is whether these are recognized and utilized appropriately by the target audience (e.g. do SMEs know who to contact and how easily can they establish the correct route), and whether resulting guidance is considered sufficient and effective. These are critical factors that impact the resulting cyber security provision in SMEs. Moreover, in addition to representing a large segment of the economy, SMEs are embedded within key and critical supply chains. Vulnerabilities emerging from SMEs, when successfully leveraged by malicious actors, result in headline breaches of large organisations, such as the National Health Service [4] and Transport for London [5], due to 3rd party compromises. However, by default, many are not positioned to play their part in this context and so need support to do so. Indeed, SMEs can be positioned very differently in terms of familiarity with cyber security and ability to act upon it. This can vary from those that feel they know little or nothing about it, through to those that know they need something but are unclear about what, or those that know what they want but not how to get there. All require a level of support, and access to related skills and expertise to provide it.

Efforts are being made at a governmental level to secure SMEs. This includes a range of local and regional initiative representatives aiding to improve their baseline cyber hygiene and resilience through grass-root efforts for awareness raising and engagement. However, little attention has been paid to the creation of peer-to-peer cyber support communities. Additionally, there is limited literature examining the design of communities in such specialized contexts that go beyond sociological or business management thought (discussed in further detail the Background section).

In parallel with the concerns on the SME side, those providing frontline support can receive queries that they are not confident or competent to address. For example, a prior survey of technology retailers had revealed a third to have less awareness around ransomware and cloud breaches [6], meaning that they must either decline or pass on the query or make a (potentially flawed) best effort attempt to help. Meanwhile, those with the technical capabilities to assist have the potential to be overwhelmed by the volume of enquiries or the extent of support required.

In response to these concerns, the authors are involved in a project that has sought to both characterise the current cyber security support landscape and then design a new approach that seeks to complement it. The resulting Cyber Security Communities of Support (CyCOS) project is a two-and-a-half-year initiative funded by the UK's Engineering and Physical Sciences Research Council (EPSRC) and linked to the Research Institute for Socio-technical Cyber Security (RISCS). It is a collaborative project led by the University of Nottingham, in partnership with Queen Mary University of London and the University of Kent, and supported by additional organisations including the Chartered Institute of Information Security, the Federation of Small Business, the Home Office, IASME, ISC2 and three regional Cyber Resilience Centres (covering the Eastern, East Midlands, and London regions of the UK).

The early phases of the work focused upon data collection from SMEs and cyber security support providers in order to assess the existing landscape, as well as to assess the coverage and clarity of existing online support materials. This work, which has been documented in prior publications [7, 8, 9] served to confirm some of the existing challenges, and provided further justification for the idea of providing an additional form of support via the community-based approach suggested in the project title. There are two related objectives for this aspect of the work:

1. To design and establish the foundations for Cyber Security Communities of Support, enabling collaborations that enhance the level and availability of specialist support available to SMEs.
2. To evaluate and refine the communities initiative via a series of pilot activities, ensuring an effective, repeatable and sustainable model for wider use.

The aim of this paper is to explain the basis of the approach that has been designed, including the concept of the communities, how they are anticipated to operate, and the related mechanisms that are provided to enable them. The discussion begins with some further consideration of the importance of SMEs in the national context, and the basis on which a community-based approach is considered suitable to reach them. This then leads into specific attention to the community approach in a cyber security context, drawing upon supporting evidence from earlier data collection and consideration of the different factors that could inform community formation. From this, the more detailed operational considerations are examined, including the roles of SME and cyber providers as community participants, and the factors that need to be addressed in terms of initiating and maintaining their engagement. Finally, attention is given to how SMEs within the communities will be supported via a Support Broker (i.e. an online platform) that enables them to socialise their questions, concerns, and other contributions. The paper concludes with thoughts on how these foundations will be used to inform a series of operational pilot communities, in order to evaluate the approach in practice.

2 Background

As already indicated, SMEs account for the vast majority of businesses in many countries and make an important economic contribution. A significant amount of research explores routes to improve cyber security practices and resilience of SMEs in the UK including their barriers to adopting cyber security [10], SME constraints [11], information transparency in supply-chains [12], and the role of service providers for SMEs to improve cyber security practices of SMEs [13]. At the same time, SMEs are playing a growing role in providing various services that can be linked to the Critical National Infrastructure (CNI). However, depending on the country and its strategic priorities, sectors that qualify as CNI are variable [14]. Perhaps consequently, the cyber security advice and guidance offered by authorities to supply-chains also varies between countries for instance, between UK, US and the European regions [15, 16]. Many countries – including the US [17], Canada [18], and Nigeria [19] - are recognizing the importance of securing SMEs to protect their CNI.

For SMEs to improve their cyber defenses or become resilient in the first instance, it is of interest to examine the sources that they are likely to interact with when trying to do so. One route within their journey is potentially through using the Internet as their first recourse. This choice is likely as it offers SMEs a wide array of information, presents them with solutions that might feel closely aligned to their challenge and, it can offer accessibility to knowledge in a technically inclined domain. To understand the information SMEs might encounter as part of this endeavor, a critical analysis was carried out to examine the coverage, completeness and clarity of online guidance documents offered by UK-based sources [7]. The findings revealed that guidance is dated and there is significant diversity in the content SMEs are presented with. This varied guidance can subsequently result in inconsistent and potentially ill-informed decision making when trying to implement organizational cyber security controls. Additionally, findings showed guidance documents in many cases provided limited information, for instance often lacking actionable steps or demonstratable successful outcomes, which can result in confusion and queries being left unresolved for the reader. Subsequent research findings within this project [8] highlighted the magnified impact from these guidance documents when SMEs are implementing advice which is amplified by their reactive needs (i.e. SMEs reaching out to advisory sources *after* an incident or a breach), limited resources and a lack of cyber security awareness and knowledge. These findings informed the design within CyCOS through the Support Broker which offers 'resources' tab to established guidance documents and affords SMEs opportunities to communicate with other members in various ways (discussed in further detail later in this section).

Further insights about SMEs' reactive needs, and the barriers to their efforts, were discovered in subsequent in-depth conversations with providers of cyber security advice [9]. The general views are that cyber hygiene amongst SMEs remains low despite efforts being made at a national level, that SMEs are considered unlikely to proactively engage with the cyber security domain, and their efforts are further hampered by aspects such as comprehension, capability, attitudes, and resources. Having said this, various activities undertaken by providers such as, interactive sessions, outreach initiatives, in-person events and regionally focused events etcetera, had been found to have a positive impact. These activities primarily include two main elements:

- **Building rapport with SMEs**. Considerations here can include various criteria such as, catering to different forms of learning, offering relatable examples, simplifying technical language, identifying relevant guidance documents that are appropriate for their queries, and capturing feedback.
- **Face-to-face interactions**. Examples include training and cyber security related events, which can have a positive impact in helping SMEs improve their baseline hygiene and resilience. Successful outcomes were noted by providers when they deliver bespoke trainings catering to SME needs.

To determine context-specific needs, organisations must be recognized with a more detailed lens than that offered by the broad term of 'SME'. Additionally, long-term exposure between SMEs and providers was believed to nurture strong relationships

between the two parties and encourage active engagement through dialogue (i.e. opportunities to directly ask questions, request help, seek guidance etcetera).

In addition to existing findings from various studies conducted in the overarching project, informal discussions were held with relevant external stakeholders who have been involved with, or lead other types of, communities in their professional careers. These discussions were held with the aim to deepen authors' understanding of designing communities (in virtual and / or real-world settings), to learn and replicate aspects that worked well, and to identify challenge areas.

Research from Johnson [20] examined online communities to define key characteristics. These include a varying level of expertise present within the group, progression in knowledge within community members and authentic tasks and communications occurring within the group's interactions. Distinctions are made within this work between designed communities (i.e. purpose based communities that exist online) and 'communities of practice' which emerge from within designed communities due to the affordances offered to users in their use (for instance, the emergence of specialized interest groups within a broader category of interest). Within the design of Cyber Security Communities of Support (CyCOS), groups are initiated by shared remits of interest for instance, in topic areas or regions (discussed in greater depth in Section 4). However, it is possible that additional groupings or specialized communities emerge from within the ones initially designed by the authors and discussed in this writing. Johnson [20] also makes a case for the various advantages and disadvantages that emerge from exclusively virtual communities that include encouragement for introvert members to participate equally to their extrovert counterparts. Good facilitation techniques can limit member withdrawal and attrition.

A study by Schou and Adarkwah [21] discussed peer-to-peer communities to develop entrepreneurial opportunities through social engagement. Findings showed online communities provide relevant developmental opportunities for individuals by providing meaningful feedback, emotional support and aspects that reduce uncertainty amongst its members. In instances investigated by them, community members were responsive (due to internet capabilities) to assist other members with sense-making when they were confused or unsure. Members also provided each other with emotional support and offered vicarious learnings which helped others when faced with ambiguity. Findings from another study [22] revealed that bonds within group members are strengthened by shared interpersonal similarities and social interactions.

Prior studies have established various design principles when creating information systems which are relevant in this writing in the context of the Support Broker (discussed in further detail in subsequent sections). For instance, authors considered the adoption of Action Research (AR) commonly used in the design of information systems [29]. Whilst data was informally captured from target audience groups at public engagements (casting votes to show preferences for various designs), AR was inappropriate due to the time resource it requires within its five research phases.

When considering the design for the Support Broker, Mansell's human capabilities [30] i.e. divergence in people's capabilities which include knowledge, habits, skills etcetera which can be developed through interactions with technologies, were also considered as part of design discussions with stakeholders. Additionally, the 'four

value-rational questions' [31] were discussed and argued by the authors as part of design meetings for the Support Broker until consensus was reached. These rationale questions are listed as follows:

- Where are we going?
- Is it desirable?
- What can be done?
- Who gains and who loses, and by which mechanism of power?

Understanding about human capabilities and the use of rationale questions which are utilized as part of information systems design, resulted in supportive evidence for the design principles discussed above to empower SMEs and segment environments within the Support Broker (and in further detail in Section 4 and 5).

3 Cyber Security Communities of Support

Part of the early work in the CyCOS project focused upon data collection from SMEs and existing support providers, in order to better understand and characterise the SMEs' needs and assess how well they are currently being served. The data collection included a series of survey and interview activities, which are already documented in prior publications [7, 8, 9]. One of the key findings from this was a clear level of concern amongst both groups that SMEs currently lack opportunities to share and discuss cyber security issues with a peer community. The following are some illustrative quotes from different participants to show these perspectives:

> *"It's very difficult to find peers that have a similar mindset to your own of a similar size that then you can have a conversation with" (SME)*

> *"What we don't know of ... is a network of people that you can share best practices with ... But there's nobody around" (SME)*

> *"One of the things I've struggled to find is like a community really ... I've looked in various places and I think because my role isn't necessarily deeply technical ... it has been difficult to do" (SME)*

> *"In terms of who would I go to talk about this, I wouldn't know" (SME)*

> "*For businesses in regions that are not specialised, it can be hard ... They don't have access to the people, they don't have the funding to pay for people, they don't have the funding to pay for the tools, that's what causes a lot of the problems" (Provider)*

> *"I see it as almost like self-help groups between businesses, where actual competition is not even factoring in there, it's just a place where everyone can get on a level pegging" (Provider)*

> *"This idea of having some sort of bridge, where SMEs are able to find us, and likewise we can find them ... being more collaborative with others is something I wish was a bit better" (Provider)*

Interestingly the quotes not only suggest an appetite from the SMEs, but also a recognition from those already supporting them that they would benefit from further routes. Indeed, the final quote also suggests that the providers themselves could also draw benefit from being linked together in a community context.

Another key finding from the data collection was that smaller organisations tend to seek information reactively and can be overwhelmed by what they find. While a myriad of resources is available, this does not equate to them being discovered, understood or used by those that need them. Again, referring to the findings from the Cyber Security Breaches Survey, the fact that only 12% of micro and small firms had heard of the *Small Business Guide* on cyber security [1] which has been available since 2018 from the National Cyber Security Centre [23], and is specifically written for this target community, demonstrates that availability does not equate to uptake. As such, having a further route through which relevant resources can be promoted and discussed would be a potentially useful means of spreading good practice.

In response to these needs, we propose the novel concept of Cyber Security Communities of Support, with the aim of guiding SMEs in understanding the need for security, how it relates to their business, and how to achieve it, while also progressively increasing the capability of the SMEs themselves and sharing the support provision across the community members. The communities are seen as a means of being able to socialize cyber security discussions within a trusted context. They deliver potential for more distributed, peer-based support, with the aim of progressively increasing the capability of the SMEs themselves and sharing the support provision across the community members. As such, participation in a community would ultimately provide a behaviour transformation mechanism for the participant SMEs.

Founded by this understanding above and considering the research findings [9] discussed earlier about the main elements that have a positive impact from activities conducted by providers, community members will share similar interests and common goals, leading to a stronger community sense and trust in sharing information and receiving advice. In practice it is envisaged that communities may be formed around different characteristics of the participating SMEs. It is important to note that whilst providers will also be part of the communities, they are there in a supporting role and thus, it is the nature of the SMEs that remains the driving factor. Thus, potential characteristics of communities considered within the project to improve cohesion are:

- **Location** – The primary option would be to group SMEs based upon their physical location. This has the advantage of then enabling community members to meet and interact in face-to-face contexts rather than just online, which is less likely to happen if they are physical disparate.
- **Sector** – SMEs may also wish to come together with others working in a common domain (e.g. construction, retail, technology), as this would give more of a shared

sense of what their specific cyber security needs might be, and a common basis on which to discuss specific threats that may affect their area of business.

- **SME size** – Given that the term SME may encompass anything from 1 to 249 people, there is potential for organizations to prefer to establish dialogue with others of a similar size. Indeed, the issues, experiences and constraints facing a sole-trader or micro business are likely to differ from those at the high-end of the medium size group. As such, size groupings based on the UK/EU standard of micro (headcount of <10), small (<50) and medium (<250) classifications would be a potential basis on which to distinguish them [24].
- **SME maturity** – This option is proposed on the basis that more established SMEs will potentially be at a different stage of their business development journey than start-ups, which in term may shape attitudes, appetite and prior experiences in relation to cyber security. As such, the nature of resulting community discussions could be quite different as their journeys continue.
- **Supply Chain** – Commonality here would be based upon SMEs being partners in the same supply chain (e.g. of a larger organization). The large business could then act as the primary source of (initial) cyber expertise to inform the community members, from which it would then benefit having raised cyber security awareness and practices amongst the businesses it depends upon. This approach links to the notion of larger organizations signing up to a Cyber Charter, as proposed in 2024's McPartland Review of cyber security in the UK [25].

The planned activity includes the establishment of a series of community pilots in order to trial the operation in practice and enable comparison of resulting experiences. Where possible, the project will facilitate face-to-face meetings to support the community building, monitor progress, and gain feedback on the outcomes and experience. The communities will be underpinned by an ethos of digital responsibility amongst the participants, and this will be emphasized in the core messaging at their formation. It is expected that SMEs will then benefit from the communities by:

- accessing community knowledge of cyber security
- receiving impartial advice and guidance from contributing security professionals
- discovering relevant resources recommended by community members
- joining (or initiating) community activities tailored to their needs and interests
- learning from other SMEs' cyber security experiences and sharing their own experiences to help others

Having outlined the concept and intent of the communities, the next section provides a more detailed examination of the underlying design and operational considerations. This involves defining operational parameters and metrics, and the baseline skills and resource requirements needed in each community.

4 Design and implementation of the Communities

Fundamentally, the community design should offer SMEs a platform whereby they can access authentic cyber security support, guidance and resources that are in line with current national guidance to support effective decision making. Additionally, these designed communities should offer opportunities for individuals to query information that they encounter in order to assist SMEs in their efforts to improve their cyber hygiene and resilience.

4.1 Overall principles

Given the intent to create a trusted and safe environment, community membership is not just a case of letting anyone in. Community formation will commence with member self-assessments informing an initial map of support provision (e.g. which source can offer what content or experience in relation to which issue). Maps will be progressively enriched as new experiences are gained within the community. Each community will incorporate SMEs alongside participants offering expertise for frontline advisory support and more specialised response capabilities.

To safeguard all community members, members who are not adhering to the code of conduct, shared at the time of signing up to the broker, will be removed by CyCOS team members who initially act as moderators within this context. The code of conduct contains general house-keeping rules which encourage members to act respectfully, honestly and ethically within their respective communities and aims to discourage disruptive behaviour which can negatively impact community wellbeing.

4.2 SME participation

Whilst CyCOS project team members will regulate the content on the Support Broker platform (with users being able to 'flag' suspicious activity or conduct), only a small proportion of the community will be providers (i.e. approximately each group will contain a 1:4 ratio e.g. 20 SMEs to 5 Providers). This also aims to empower SMEs as a majority grouping within each community.

To implement aspects of trust and safety, SME status will be checked by CyCOS team members at the time of sign-up. This includes SME's listing and status on the 'Companies House' [26] website (UK's registrar of companies) to verify company identities. Additionally, through the Support Broker (discussed in greater detail below), email account verification of users will take place when users join the community.

4.3 Provider participation

Providers will also be asked to declare their areas of expertise and share any supporting credentials at the sign-up stage which will subsequently be verified by CyCOS team members. Providers will also be requested to select a suitable role within the community as either a provider or an SME i.e. if they are representing their organization

or are acting in an independent or volunteer capacity. This will limit any assumptions being made on behalf of members since individuals who might be in a cyber security or IT related role within their organization can be representing the interests of their SME organization.

Preliminary efforts when engaging target audiences for pilots, for instance a CyCOS exhibition stand at the SME XPO 2025, has generated a healthy interest from providers who have been eager to share their expression of interest. This appetite amongst providers, i.e. to network with SMEs and other providers, was also garnered from findings from earlier research conducted by the authors [9]. This enthusiasm demonstrated by providers initially serves as a predominant motivator for them to participate and engage with the designed pilots. One insight from informal discussions with stakeholders indicated the need to crystallize the role providers play within communities. Providers, who can potentially come from organisations that provide commercial cyber security services to SMEs, can rapidly become a majority population within the user base. Thus, any providers being accepted into CyCOS must adhere to providing impartial, independent advice at the time of their admittance to the community. Additionally, provider roles are voluntary in their nature and thus must be performed ethically (i.e. providing impartial, independent and non-competing advice).

4.4 Provisioning communities and maintaining engagement

Based on insights discussed in the Background section above, CyCOS are designed to offer a hybrid approach (i.e., virtual and in-person events) to realize these benefits and encourage active engagement. Face-to-face events in real-world settings will be offered to SMEs participating in the pilots with various objectives such as those that offer to raise awareness and knowledge about cyber security for example, an ‘Exercise in a Box’ activity offered by affiliated partner NCSC [27], to those that celebrate national seasonal festivities. These sessions will also capture feedback from pilot participants about individual experiences to highlight areas that can replicate success or identify learning opportunities. Simultaneously, the Support Broker can cater to individual needs of learning, and facilitate dialogue (between providers and SMEs, and within peer-to-peer groups amongst SME groups) and up-skilling incentives will continue to be offered to participants through affiliated project partners such as, ‘Certified in Cybersecurity’ online certification offered by affiliated partner ISC2 [28].

The presence of cyber security professionals (or ‘providers’) within these communities is also designed to provide SMEs with a medium to ask questions, assist in simplifying technical language and concepts, and provide help with identifying relevant guidance documents that are best suited to their needs – resulting in potentially establishing strong inter-relations within and across the two parties. Prior to joining the pilots, SME members will be given the opportunity to express interest in the type of community they would prefer to join (e.g. regional or sectorial communities, SME maturity, and/or if they are supply-chain entities, all aspects that they most identify with to offer them a group which resonates with their own organizational identity). Furthermore, discussions initiated by SMEs about their lived experiences or challenges

will provide organic examples that are relatable to other members within their respective group.

Our preliminary findings suggested that in addition to individual learning needs (including independent learning) and establishing the relevance of security advice to their contexts, SMEs can be further supported in their cyber security pursuit through incentivization. Thus, CyCOS are designed to offer participants cyber security materials, courses and events that upskill existing talent within organisations. For instance, through our affiliated partner, ISC2, as part of this project participants are offered a free 'Certified in Cybersecurity' course for their early-career employees as part of their professional development within this domain. This up-skilling will also provide each community with a varying level of expertise amongst SMEs to supplement providers who are qualified and / or experienced cyber security professionals.

The approach discussed above is founded by the project's published and preliminary findings and shown in Fig. 1 below.

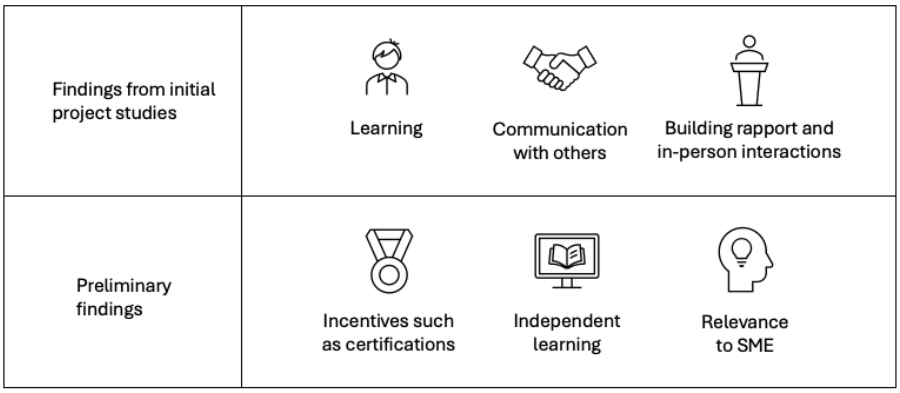

Fig. 1. Findings from earlier research studies to inform the design of CyCOS

Informal discussions with stakeholders highlighted the importance of autonomous, self-regulating communities to achieve successful outcomes. Consequently, the SME role will be designed to encourage them to be proactive for instance, through identifying communities they would like to join at the time of signing up (discussed above), requesting them to identify cyber security topics they would like to learn more about, ask questions or share their daily experiences. To supplement this effort, CyCOS team members will share information relevant to each community (for instance, with relevant news stories, regional initiatives, relevant research findings, domain developments etc.) and remind inactive members to engage within their groups.

In addition to the role of providers and SMEs, equal thought was paid in discussions to the role of the community itself, which is to facilitate cyber security discussions with an aim to improve SMEs' baseline hygiene and resilience. CyCOS is designed to enable discussions to achieve stated aims but is not a creator of advice. Instead, the communities can act as a channel to promote existing good practice, such as the guidance offered by National Cyber Security Centre. As an enabler, it provides a

platform through which different voices within the community are sources of advice to varying degrees i.e. CyCOS team members facilitating workshops and events with recognized professionals from partners, independent providers within the communities acting as volunteers, and the SMEs themselves through sharing information and their experiences.

Finally, discussions highlighted 'outreach activities' as foundational work to create successful communities. A main aspect of this outreach is through affiliated partners. Leveraging existing partnerships were believed to improve recognition of an initiative and stimulate participation from target groups. CyCOS aims to utilize relevant partnerships and its affiliations with regional bodies and those who operate in specific sectors to initially promote its emergence. Outreach activities can also assist in gaining initial momentum and traction to engage relevant SME audiences in the first instance. CyCOS has initially leveraged public expositions and existing partners to organize the delivery of the first piloting communities. Once pilots commence, CyCOS team members are designed to play an assistive role to further this aspect through propositioning community discussions and scheduling period emails.

Based on extant literature, findings from our overarching project's research studies and insights gained from discussions with various stakeholders, Fig. 2 inspired from [20, 21] below, depicts the principles underpinning communities of support. Members are able to operate with feelings of safety and trust within the designated community, and the overarching expectation is that community knowledge is greater than individual knowledge.

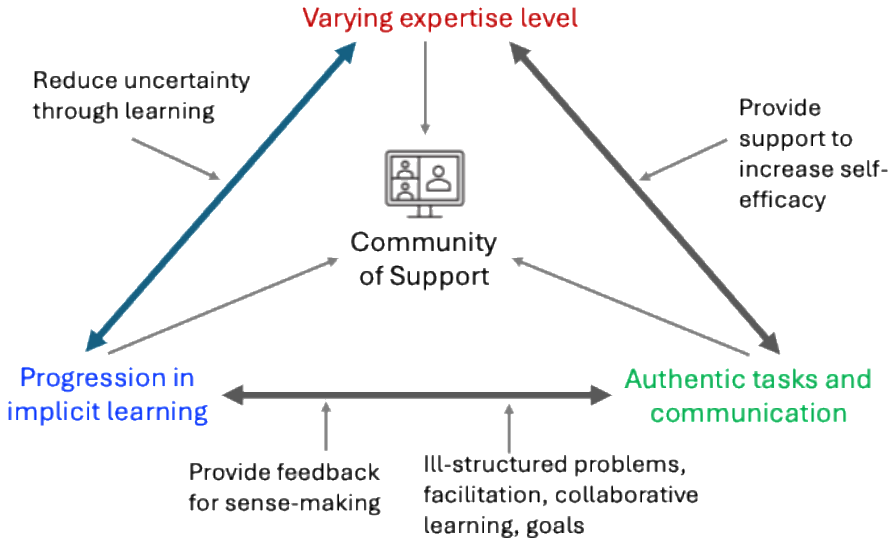

Fig. 2. Underpinning principles used to design CyCOS

Communities have three main features which are dynamic and responsive to each other i.e. they exhibit authentic tasks and communications, there is a varying level of

expertise within the community, and there is implicit progression in learning amongst members. Varying level of expertise available to support tasks and communications within communities will provide support (technical and emotional) to improve self-efficacy amongst members. This is supplemented by CyCOS team members' efforts (discussed above). For instance, members requesting assistance or reading about others' experience might subsequently improve their self-belief and confidence in their own abilities. Communications in virtual and physical settings with peer-to-peer groups and providers will implicitly contribute to members' knowledge and learnings. This can potentially be demonstrated via analytical tools for the Support Broker to reflect ill-structured problems, collaboration and engagement between members, and posts that provide feedback to proposed solutions. Similarly, a varying level of expertise within a community can potentially allow members at varying knowledge levels and with individual forms of learning to improve their cyber security understandings. This understanding, knowledge and awareness can reduce uncertainty experienced by SMEs when they are trying to improve their cyber hygiene or resilience. At any given point, for the community to function effectively, the overall knowledge within the group must be larger than that held by one individual within the same group to facilitate equal learning opportunities and interactions.

Since cyber security domain contains sensitive data and SMEs sharing specific organizational challenges can risk exposure, communities must be safe and deemed trustworthy by its members. To instill safety and trust amongst members (i.e. people are who they say they are and are presenting their skills accurately), the CyCOS team members will perform initial manual checks via public domains prior to admitting members and verify user accounts via automated emails through the Support Broker. Members will not be able to change key information such as their names or email IDs after the verification check is complete. Data documenting user activity will also be securely held as part of back-ups to keep activity logs in case information is removed from the Support Broker.

In keeping with earlier findings, face-to-face events will also be periodically facilitated by CyCOS team members to promote strong rapport amongst community members and foster trust. The Support Broker platform supporting the virtual aspects of the communities is enabled by the Internet.

5 Support Broker platform

One of the key foundations for the communities is the creation of an online Support Broker, enabling the SMEs to identify support needs and contact advisory sources positioned to help them (which, as the community develops and grows in experience, may include peer support from other SMEs). The Support Broker is an online platform enabling SMEs to submit support requests and other members to provide responses (ranging from direct advice to facilitating linkage to specialized support).

The original plan was for the project to develop a fully bespoke tool that would enable access to online support, and some initial exploratory work was undertaken in this direction. However, it was realised that the development effort required would

outweigh the likely benefits when compared to using an existing online forum and discussion platforms. A bespoke tool would require ongoing maintenance that would then require commitment and support beyond the initial funded period of the project, whereas the selection of a suitable third-party platform would ensure this happened naturally, and there would be a wider community of platform users to help encourage longevity of support.

The resulting Support Broker is based on the open-source community building and discussion platform, Discourse, shown in Fig. 3 below.

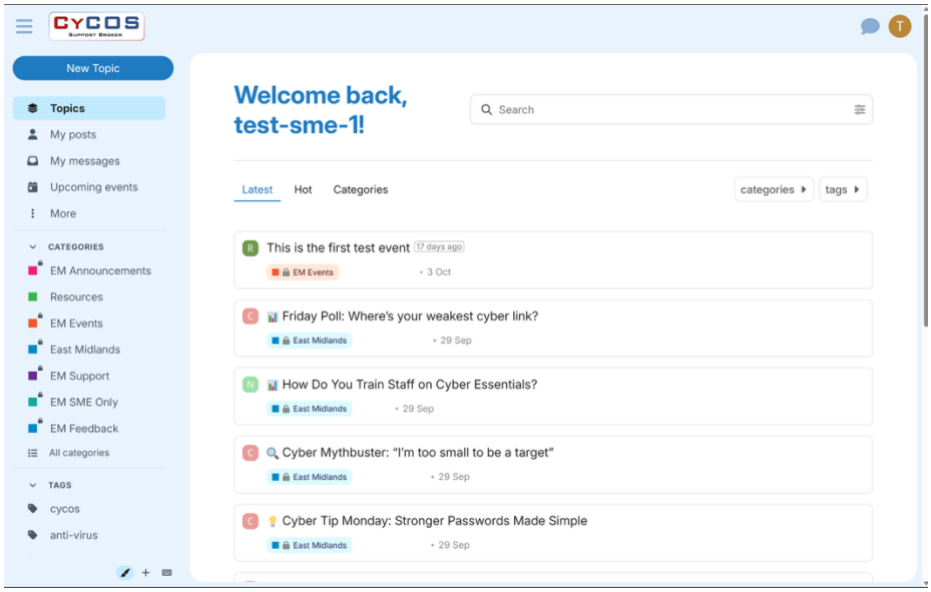

Fig. 3. An image of the Support Broker as viewed by a participant within a community

There will be two primary user groups initially to start the communities (i.e. SMEs and Providers) with an option to create more user groups later on. Sign-ups to the community will be by invitation only. CyCOS team members will initially act as the administrators and moderators of the platform. They will designate users to their correct group and give them the appropriate role-based permissions and tags, e.g. SME or Provider. Upon signing up users will be directed to the CyCOS welcome message, a general introduction on how to navigate the forum, and the community's code of conduct.

The Support Broker, enabled via Discourse platform, will be segmented – potentially into at least three environments –with groupings based on distinct and potentially collegial features such as location, sector, SME size, SME maturity and supply-chain. These decisions will be determined by users at the time of sign-up as discussed earlier. Each of these groups informing their respective community will be architecturally identical with an announcement category (for the CyCOS team members), security news, general discussions and support. As pilots progress, new features to support

community activities and engagement can be added. SMEs will be able to raise topics of interest or respond to an existing discussion. Providers, who are professional cyber security experts, can then share relevant advice or ask SME users for further information. This can help foster a gradual building of SMEs' cyber security capability. For the experts the platform will offer networking opportunities within focussed communities.

SME users will be able to interact with and access targeted expertise within their community of support. They will also have the ability to provide peer-to-peer support to others. For example, if they are in a regional community they will be able share local threat intelligence and discuss their region's infrastructure. In an industry-focused community, they will be able to discuss sector-specific cyber security challenge and regulatory and compliance issues. For a supply-chain community, discussions can involve vendor-client cyber security requirements or risk assessments.

The Support Broker platform is designed to be a scalable model and will be able to support multiple community types. These community types can become self-sustaining communities of support with minimal oversight needed in line with the earlier discussion about autonomous, self-regulating communities to achieve successful outcomes. There is also a Data Explorer module which will allow team members to make custom SQL queries against the live database. At the same time, it should be noted that the Support Broker, and indeed the wider community approach, will give participants control over what level of information they share and to whom it is available, in order to respect the business sensitivity that may be linked to some support requirements.

6 Evaluation of the Communities

As discussed in Sections 4 and 5 above, the communities are designed to be in a hybrid format which utilises in-person engagements as well as online interactions facilitated by the Support Broker. To analyse and reflect on the pilots' delivery, data will be collected and evaluated to support conclusions.

Various metrics will be captured from in-person events metrics such as, attendance, qualitative feedback, and audience participation. Additionally, through self-assessment forms participants will be asked to share their experiences at three specific points: 1) Prior to the commencing of pilots, 2) at the midway point and, 3) at the end of pilots. Feedback forms will contain qualitative and quantitative questions which seek to capture their motivations for being part these communities, any perceived benefits or challenges they have encountered, change in their cyber security knowledge, and perceived variance in organisational security levels. These qualitative self-assessment forms can provide impact generated from these designed communities and offer insights to potential challenges for them to be autonomous and self-regulated when being scaled up.

Additionally, during pilots CyCOS team members will be able to collect analytical data from the Support Broker. These data points can include a range of activity related metrics such as, topics discussed by users, views to a post, likes, replies etcetera. This

quantitative dataset can provide further evidence of engagement amongst participants when seeking support to improve their security or resilience and provide insights to responsiveness amongst the community when SMEs endeavour to do so.

7 Conclusions and future plans

The next stage of the work is to test the community approach in practice, via a series of pilot groups, with the aim of running at least three communities and monitoring their operation for a period of at least three months. While addressing SMEs in general, the research is particularly interested in small and micro firms, where there is greatest likelihood of needing additional support combined with the least potential to have the resources to enable security to be outsourced.

During the operational period, communities are expected to interact largely via online communications, including the use of the Support Broker to enable and maintain activity. The project team will maintain oversight and engage as necessary throughout the period, including initially providing the role of community moderators as needed. It is anticipated that one of the key findings from the pilots will be to expose the challenges around achieving initial and sustained engagement from the community members.

The conduct of the community pilots will lead to analysis and reflection, considering both the operational metrics (e.g. queries submitted and resolved) and participants' feedback on their pilot experience (captured during reflection meetings). Both aspects will feed into an evaluation of the pilots, and the refinement and finalization of the operational guidance to support the establishment, operation and sustainability of such communities beyond. As part of future plans for the communities to be autonomous and self-regulating, providers and SME users will be enabled to act as leaders and champions of the Support Broker platform. This can include aspects such as members being selected to perform administrator or moderator roles within their respective communities or members contributing nominal monetary amounts to sustain the operational costs such as those associated to the broker. It is hoped that this will inform the potential for wider uptake of the Community of Support concept, providing a replicable model with applicability beyond the initial UK context.

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

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

1. DSIT (2025). Cyber Security Breaches Survey 2025. Department for Science, Innovation and Technology, 10 April 2025. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025
2. OECD (2022). SMEs and entrepreneurship. Organisation for Economic Co-operation and Development. https://www.oecd.org/en/topics/policy-issues/smes-and-entrepreneurship.html, last accessed 2025/8/24
3. FSB (2025). UK Small Business Statistics. National Federation of Self Employed & Small Businesses Limited. https://www.fsb.org.uk/media-centre/uk-small-business-statistics
4. NHS Homepage, https://www.england.nhs.uk/2024/06/synnovis-cyber-attack-statement-from-nhs-england/, last accessed 2025/08/27
5. Transport for London Homepage, https://tfl.gov.uk/fares/free-and-discounted-travel/cyber-security-incident, last accessed 2025/08/27
6. Koshnaw, B. and Furnell, S. (2022) "Assessing cyber security consumer support from technology retailers", Computer Fraud & Security, March 2022. https://doi.org/10.12968/S1361-3723(22)70560-X
7. Khan, N., Furnell, S., Bada, M., Nurse, J. R. C., & Rand, M. (2024, July). Assessing cyber security support for small and medium-sized enterprises. In International Symposium on Human Aspects of Information Security and Assurance (pp. 148-162). Cham: Springer Nature Switzerland.
8. Khan, N., Furnell, S., Bada, M., Nurse, J. R. C., & Rand, M. (2025). The hidden barriers to cyber security adoption amongst Small and Medium-Sized Enterprises. Information & Computer Security.
9. Khan, N., Furnell, S., Bada, M., Rand, M., & Nurse, J. R. C. (2025). Investigating the experiences of providing cyber security support to small-and medium-sized enterprises. Computers & Security, 154, 104448.
10. 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.
11. 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.
12. Lewis, R., Louvieris, P., Abbott, P., Clewley, N., & Jones, K. (2014). Cybersecurity information sharing: A framework for information security management in UK SME supply chains.
13. Cartwright, A., Cartwright, E., & Edun, E. S. (2023). Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies. Computers & Security, 131, 103288.
14. Mbanaso, U. M., Makinde, J. A., & Kulugh, V. E. (2023). A methodological approach for characterisation of critical national infrastructure. International Journal of Critical Infrastructures, 19(2), 172-197.
15. Pemmasani, P. K. (2023). National Cybersecurity Frameworks for Critical Infrastructure: Lessons from Governmental Cyber Resilience Initiatives. International Journal of Acta Informatica, 2(1), 209-218.
16. Topping, C., Dwyer, A., Michalec, O., Craggs, B., & Rashid, A. (2021). Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks. Computers & Security, 108, 102324.

17. Melnyk, S. A., Schoenherr, T., Verter, V., Evans, C., & Shanley, C. (2021). The pandemic and SME supply chains: Learning from early experiences of SME suppliers in the US defense industry. Journal of Purchasing and Supply Management, 27(4), 100714.
18. Quigley, K. (2013). “Man plans, G od laughs”: Canada's national strategy for protecting critical infrastructure. Canadian Public Administration, 56(1), 142-164.
19. Obokoh, L. O., & Goldman, G. (2016). Infrastructure deficiency and the performance of small-and medium-sized enterprises in Nigeria's Liberalised Economy. Acta Commercii, 16(1), 1-10.
20. Johnson, C. M. (2001). A survey of current research on online communities of practice. The internet and higher education, 4(1), 45-60.
21. Schou, P. K., & Adarkwah, G. K. (2024). Digital communities of inquiry: How online communities support entrepreneurial opportunity development. Journal of Small Business Management, 62(5), 2364-2395.
22. Fiedler, M., & Sarstedt, M. (2014). Influence of community design on user behaviors in online communities. Journal of Business Research, 67(11), 2258-2268.
23. NCSC (2018). Small Business Guide: Cyber Security, National Cyber Security Cen-tre, 15 November 2018. https://www.ncsc.gov.uk/collection/small-business-guide, last accessed 2025/8/24
24. Government Commercial Function (2023). Supplementary information: Small and Medium-sized Enterprises definition. 11 April 2025. https://www.gov.uk/government/publications/procurement-act-2023-short-guides/supplementary-information-small-and-medium-sized-enterprises-definition-html, last accessed 2025/8/24
25. DSIT (2024). “McPartland review of cyber security and economic growth”, Depart-ment for Science, Innovation and Technology, 6 February 2024. https://www.gov.uk/government/publications/mcpartland-review-of-cyber-security-and-economic-growth, last accessed 2025/8/24
26. Companies House. https://www.gov.uk/government/organisations/companies-house/about. Crown copyright.
27. National Cyber Security Centre Homepage, https://www.ncsc.gov.uk/section/exercise-in-a-box/, last accessed 2025/08/27
28. ISC2 Homepage, https://www.isc2.org/certifications/cc, last accessed 2025/08/27
29. Lau, F. (1997, January). A review on the use of action research in information systems studies. In Information Systems and Qualitative Research: Proceedings of the IFIP TC8 WG 8.2 International Conference on Information Systems and Qualitative Research, 31st May–3rd June 1997, Philadelphia, Pennsylvania, USA (pp. 31-68). Boston, MA: Springer US.
30. Mansell, R. E., & Silverstone, R. (1996). Communication by design (pp. 15-43). Oxford: Oxford University Press.
31. Flyvbjerg, B. (2001). Making social science matter: Why social inquiry fails and how it can succeed again. Cambridge university press.