University of Kent

Kent Academic Repository

Rand, Matthew, Khan, Neeshe, Furnell, Steven, Bada, Maria, Nurse, Jason R. C. and Herkanaidu, Ram (2026) *Analysing the cyber security support journeys of small and medium sized organisations.* In: International Conference on Availability, Reliability and Security (ARES). Lecture Notes in Computer Science . pp. 479-496. Springer ISBN 978-3-032-35585-0. E-ISBN 978-3-032-35586-7.

Downloaded from

https://kar.kent.ac.uk/115811/ The University of Kent's Academic Repository KAR

The version of record is available from

https://doi.org/10.1007/978-3-032-35586-7_26

This document version

Author's Accepted Manuscript

DOI for this version

Licence for this version

CC BY (Attribution)

Additional information

For the purpose of open access, the author(s) has applied a Creative Commons Attribution (CC BY) licence to any Author Accepted Manuscript version arising.

Versions of research works

Versions of Record

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

Author Accepted Manuscripts

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

Enquiries

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

Analysing the Cyber Security Support Journeys of Small and Medium Sized Organisations

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

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

Abstract. Small and medium-sized enterprises (SMEs) frequently find themselves as exposed to cyber security threats as larger organisations. However, most SMEs are not experts in cyber security and therefore need additional support to enhance their cyber resilience. Furthermore, although they may seek related support, there is minimal knowledge about how they approach this or how effective the support is. This study aimed to understand the support journeys that SMEs pursue when they have a question or concern about cyber security, sampling both SMEs and cyber security providers. Both groups were asked to record each time they had a support journey instance, to outline factors such as what the instance involved, how satisfied they were with the support, and what the resulting outcomes were. This enabled comparison of how support was accessed, experienced, and resolved across cases, from the initial trigger for support through to the outcome. A series of practical recommendations are provided within this paper following the analysis of these support journeys, to consider how both SMEs and providers can benefit from the support journey experience. The experiences also highlight some of the broader challenges of supporting SME engagement with cyber security, including the constraints they face in terms of time and understanding.

Keywords: Cyber Security, Cyber Security Support, Cyber Security Behaviour, SMEs, Cyber Hygiene.

1 Introduction

Small and medium-sized organisations (SMEs) are continually facing similar cyber security threats as large organisations, with approximately 50% of small organisations and 67% of medium organisations reporting that they have identified breaches or attacks in the last 12 months [1]. This increase in threats is partly because SMEs are increasing their use of online technology, which is creating a growing online attack surface.

Smaller organisations tend to have fewer formal processes and procedures to combat cyber security risks [1]. SMEs can undertake a number of simple but effective measures to prevent a cyber security issue, such as having minimum requirements for passwords, installing security patches in a timely manner, implementing multi-factor authentication and having an automatic backup system in place [2]. SMEs appear to be generally concerned about cyber security, however very few know how to implement the necessary security controls to effectively address the risks, with conflicting and confusing advice on how to tackle the issues generating this uncertainty [3].

SMEs are heterogeneous in their nature, as although they can be categorised together due to their size, sector, and age, they vary in many ways. When analysing SME size, a very small organisation (e.g. sole trader or micro organisation with under 10 employees) may have different needs to a larger SME with more employees. Such organisations may also have different levels of resources (e.g. financial) to support their pursuit of cyber security despite having the same security needs [4]. Although it may appear obvious that all SMEs should engage in cyber security, many are not [5], with SMEs not perceiving it as a risk they should take seriously [6], or not having the required awareness [7] or knowledge and understanding [8] to realise they could be doing more to ensure their organisation is cyber secure.

Understanding how SMEs can improve their cyber resilience is therefore key, including how they can find the appropriate support that will meet their needs. This paper examines SMEs' cyber security support journeys, defined as the progression from an initial support trigger, through subsequent interactions and decisions, to the reported outcome.

2 Related Works

When SMEs have a cyber security question or concern, there are a variety of avenues they can take. Given the continual advancement of the internet and technology, one option is to source support online (i.e. with minimal personal contact) [9]. SMEs may tend to have financial resource constraints compared to larger organisations and these online resources could provide a cost-effective way of seeking appropriate support [10]. Online search engines such as Google enable SMEs to easily access resources to support them, such as those located on the UK National Cyber Security Centre (NCSC) website [11]. There are, however, a wide variety of resources available to SMEs online, with one of the fundamental issues for SMEs being where to initially find the appropriate information and, once found, how to navigate the volume and variety of sources that they have access to [12]. This challenge is consistent with broader work showing that online security and privacy advice is extensive and often difficult to prioritise, leaving users with many possible actions but limited clarity about which are most important [13]. SMEs may lack specialised information security or IT departments that have the expertise to know the true cyber security problem affecting the SME and the awareness and knowledge to know where the most appropriate resources are to meet their needs [14]. This challenge is not limited to cyber specific guidance alone, as wider work on

SME digital transition also shows that SMEs often require flexible and targeted support to help decision makers understand and act on technical change [15].

The second method that SMEs may look to seek cyber security support is to have direct contact with a cyber security provider (e.g. a managed service provider). This provider may have been an existing provider of IT services for the SME or may be a new provider for the specific concern or question. Recent work suggests that these relationships are shaped not only by technical need, but also by organisational context, differing expectations, and the wider governance arrangements within which SMEs and providers operate [16]. Related research also indicates that SME cyber security engagement can be complicated by financial constraints, uneven levels of cyber security understanding, and misaligned roles and responsibilities between SMEs and third-party providers [17]. More broadly, recent review work continues to show that SMEs remain especially exposed to cyber threats because of resource constraints, limited awareness, and insufficient protective measures, reinforcing the need for practical and well-targeted support routes [18]. When seeking support, SMEs may also be proactive (e.g. risk management) or reactive (e.g. taking action following an incident) in their behaviour. One of the fundamental issues for SMEs is where to initially find the appropriate information and, once found, how to navigate the volume and variety of sources that they have access to [19]. Having such a variety of sources could potentially lead to ill-informed decision making by the SME [20]. Understanding how an SME navigates the support landscape is therefore key in understanding whether they are successfully navigating their support journey routes. Although prior work has examined SME cyber security challenges, online advice, governance, privacy, awareness, and the role of providers, less is known about how SMEs move through support as an unfolding journey in practice, from the initial trigger for support through to the interactions, decisions, and outcomes that follow. It is this understanding that is the focus of this paper.

The focus of this research involved capturing details of what instances happen during the resulting support journeys (i.e. from start to finish, including what triggered the need for support, who was contacted, what support was provided and what the outcome was), alongside insights into aspects such as challenges encountered and lessons learned. Resulting case examples of selected support incidents will enrich the understanding of SME and provider experiences, with deeper insights into practical challenges and constraints on each side.

3 Method

The current study adopted a comparative case-based qualitative approach, informed by case study research [21], to examine how SMEs seek cyber security support and how cyber security providers deliver that support. The research study procedure was divided into four phases, as illustrated in Figure 1. Phase 1 established a common understanding of the research focus. Phases 2 and 3 concern data collection and construction of the actual support journeys, whilst Phase 4 focused on the analysis of results, identifying key clusters and recommendations across the support journeys.

3.1 Phase One

The research team undertook two meetings and an additional discussion with the project advisory board in early 2024 to establish the primary areas of focus for the study. Within these meetings it was established that both SMEs and providers should 1) provide insight on their support journeys qualitatively and 2) be able to provide insight at the time, or soon after, the support journey took place. Following these meetings, it was decided that the focus of the study instruments would be on the 1) scenario that triggered the need for support; 2) topic of support; 3) sources used; 4) type of interaction; 5) description of the instance/interaction; 6) satisfaction level; 7) other supporting information; and 8) reflection on the overall support experience.

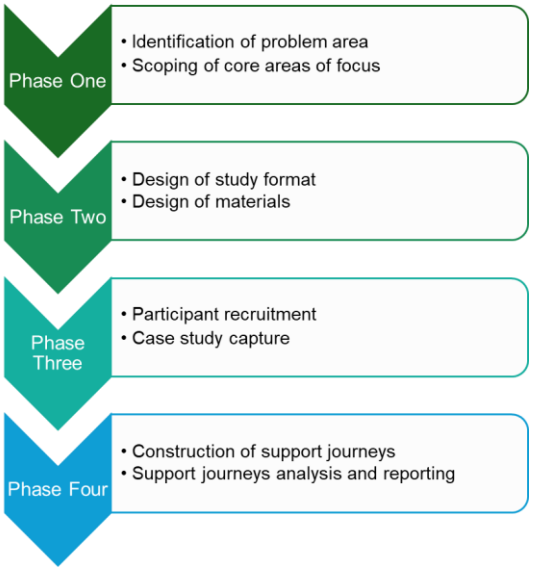

Fig. 1. The four phases of the support journey procedure.

3.2 Phase Two

The support journey data was collected through an online form. Both SMEs and providers were asked to record each stage of the support journey in an individual submission, described to participants as an instance. Towards the end of each instance, participants were asked whether the instance was the end of the support journey. If this was not the end of the support journey, participants were asked to revisit the form to submit the next stage of the support journey. If the instance was the end of the support journey, participants were asked to evaluate the support journey experience.

Both SMEs and providers were given an ID to be used for each instance and were also asked to name their respective support journeys. Two separate forms were used for providers, depending on whether the interaction with the SME was one-to-one or within a group setting.

The SME form captured the participant ID and journey name, the trigger for support, the cyber security topic, sources used, type of interaction, a short description of what happened, satisfaction with the instance, and any lessons learned or supporting information. Where participants indicated that an instance represented the end of the support journey, they were also asked to report the overall outcome, overall satisfaction, what worked well, lessons learned, challenges faced, and any further reflections. The provider forms covered the same core topic areas, with additional questions relating to the nature of contact, who initiated the interaction, and who was involved.

3.3 Phase Three

After ethical approval from the University ethics committee, 21 SME organisations and 24 cyber security providing organisations were recruited into the study. The participating SMEs represented a diverse range of sectors. The sample included organisations from professional, scientific and technical services (n = 6); information and communication (n = 4); education (n = 3); health and social care (n = 3); retail and wholesale (n = 2); administrative and support services (n = 2); and transportation and storage (n = 1). Prior to being recruited, participants were sent a study information sheet and a consent form to complete, sign and return to the study research team. Upon recruitment into the study, participants each had a one-to-one video call with a member of the research team as an introduction to the research study and as an opportunity to ask any questions about their role in the study. Each participant was recruited into the study on a rolling basis for a three-month period between June 2024 and September 2025. 38 SME instances and 39 provider instances were submitted from a total of 12 SMEs and 14 Providers. As the study relied on participants recording support journey instances over time, sustained engagement was required throughout the data collection period, and reminder emails were sent where appropriate to encourage continued completion of submissions. Multiple submissions could relate to different stages of the same ongoing journey, because participants were asked to submit a new form each time the support journey progressed. As a result, the submitted instances were later collated into broader support journeys during analysis.

3.4 Phase Four

First, all submitted instances were collated and organised into support journeys by grouping together submissions that referred to the same journey name and issue. This enabled individual form submissions to be reconstructed into broader support journeys that captured the progression of support seeking over time.

45 organisations were recruited into the study, comprising 21 SMEs and 24 cyber security providers. Submissions were received from 12 SMEs and 14 providers, generating 77 submitted instances in total. These instances were then grouped by participant ID, and journey name to reconstruct broader support journeys. From this reconstructed dataset, eight information-rich journeys were selected for detailed presentation and used as the basis for the cross-case synthesis.

The full set of submitted journeys was reviewed by the first author. Eight support journeys were selected for detailed presentation for this paper, because they contained sufficient detail on the trigger, support route, interaction, outcome and reflections to allow meaningful comparison.

The selected support journeys were analysed through a comparative case-based approach informed by case study analysis [21]. Each time support was sought was treated as a separate case and examined several times to identify its key features, such as the trigger for support seeking, the support sought or provided, the nature of the interaction, the challenges encountered and the reported outcomes. Journeys were compared across cases to identify their commonalities and differences in access to, delivery of and experience with cyber security support. Iterative review was used to identify recurring patterns across the journeys during the cross-case comparison. Similar cases were grouped to identify the common factors that influenced support experiences.

From this cross-case comparison, broader patterns were synthesised into a set of practical learnings and recommendations. These recommendations were developed by identifying features that appeared to contribute to more effective support experiences, alongside recurring barriers and frustrations reported across cases. Table 1 provides a four-phase overview of the study design.

Table 1. Four-phase overview of the study design

Phase	Purpose	Main activity	Output
1	Scope and instrument design	Meetings with the research team and discussion with the project advisory board to refine the study focus and the core areas to be captured in submissions.	Agreed study focus and data collection domains for the forms.
2	Data collection setup	Development and deployment of online forms for SMEs and providers to record individual support journey instances over time.	Form-based submissions capturing triggers, support topics, sources, interactions, satisfaction, outcomes, lessons learned, and challenges.
3	Recruitment and participation	Recruitment of SMEs and cyber security providers, onboarding calls, rolling participation over a three-month period, and submission of instances as journeys progressed.	21 SME organisations, 24 cyber security providing organisations, 38 SME instances, and 39 provider instances.
4	Data preparation and comparative analysis	Collation of submitted instances into broader support journeys, selection of information-rich journeys, within-case review, and cross-case comparison to identify recurring patterns.	Eight illustrative support journeys and a cross-case synthesis of learnings and practical recommendations.

4 Results

A total of eight support journeys are described in this section. Journeys were selected on the basis that they contained multiple stages or detailed reflections on the support process, including the trigger for support, the type of interaction and the outcome. The described support journeys are in the areas of Secure Sockets Layer (SSL) Certification; Incident Preparedness; Data Protection; Incident Response; Access Management; Cyber Essentials Certification; Risk Management; and Phishing Incident. These support journeys were submitted by both SMEs (support journeys A–F) and cyber security providers (support journeys G and H).

4.1 Support Journey A - SSL Certificate

This support journey focuses on a sole trader running an audiology/lip-reading organisation who needed to renew the SSL certificate for her website. As the website supported online transactions, the SSL certificate was important for keeping customer information and transactions secure.

The issue was first identified by a customer, who informed the sole trader that the SSL certificate had expired. The sole trader had not been aware of the expiry and explained that she had "*limited tech knowledge to resolve the issue*". She therefore contacted the website hosting company, but support was only available between 9am and 5pm, delaying the resolution. On the same day, she also received an email from the hosting company explaining that they were "*transferring their hosting business*", which prompted her to consider whether she needed to review who should host her website. At this stage, the sole trader was very unsatisfied with the experience. Twenty days later, she reported that she was "*satisfied website is available again*" but remained "*worried that I'll have to do it all again next year*", particularly because the hosting company was being transferred to another provider. She also described the difficulty of working across two companies and explained that technical support may suggest solutions that do not match the specific problem, such as changing server names. She noted that "*information on the web never quite fits the scenario you are trying to sort out*". As a result, she wanted to find a hosting company that could provide knowledgeable, as-needed support. She also felt it would be useful if the hosting company shared clearer knowledge about what needed to be done, so she could manage future certificate renewals herself.

This journey shows how limited warning, support availability and guidance can delay resolution and create dissatisfaction for SME website owners.

4.2 Support Journey B - Incident Preparedness

Many SMEs take cyber security action reactively, after a specific trigger or prompt, rather than proactively. In this support journey, however, the co-owner of a website development organisation with approximately 20 employees took a proactive approach after receiving the NCSC newsletter and a link to the British Library cyber attack re-

view. The review provided an overview of the cyber attack on the British Library in October 2023 and examined its operations, future infrastructure, risk assessment and lessons learned. The co-owner described that "*the NCSC newsletter included a link to guidance on communications in the event of a cyber incident. We read that guidance and followed the link to the British Library cyber attack review. (It) furthered our understanding of comms in the event of cyber security*". The next stage involved discussions amongst team members after reading the review: "*this was distributed to key team members involved in cyber security for a follow up discussion on what we might learn from this*". The co-owner subsequently found that "*the case study gave us some food for interesting conversations*".

This journey shows how NCSC guidance can prompt proactive reflection and internal discussion, particularly where SMEs may not routinely prioritise cyber security during day-to-day work.

4.3 Support Journey C - Data Protection

The IT manager in one SME described seeking a new provider to support data protection and business continuity planning. Before her appointment, the internal auditor had raised business continuity as an issue and recommended business impact assessments. The IT manager completed these assessments, identified key business processes and systems, reviewed disaster recovery arrangements, and contacted vendors for testing evidence and cost proposals.

Although she received proposals from two cyber security providers, neither could be progressed. In the first, the provider could offer testing evidence, but the SME's current Managed Service Provider (MSP) had removed a backup service for on-premise infrastructure without replacing it for cloud services. Disaster recovery was also available only at additional cost. In the second, there was no mention of disaster recovery, and the SME was still awaiting a security configuration review. Because of this mismatch between what the SME needed and what providers offered, the SME paused its search for a provider.

As the IT manager described, the process was useful internally in "*identifying key risks, sequencing of recovery and engaging the senior team*". However, the "*time taken to get these proposals was too long from vendors*" and they had "*expected them to be off the shelf, given the prevalence of cyber incidents*". The IT manager also felt she was initiating what was needed, rather than being advised and guided by the provider.

4.4 Support Journey D - Incident Response

In this support journey, the Head of Information Technology Solutions of a logistics company with approximately 200 employees described the support required from an MSP following a potential incident. The first stage involved a "*Customer contacting us saying they had an email from our MD (Managing Director) advising of a change in our bank details*". The SME then contacted its MSP, which "*took the lead on investigating what might have happened, changing passwords and resetting MFA (multi factor authentication)*".

This SME had worked with the MSP for many years, allowing the MSP to develop knowledge of the organisation and respond efficiently. The Head of Information Technology Solutions described this by saying, "*I was able to pass everything off to the MSP and they dealt with the issue for me, I simply needed to make a phone call to alert them*". The organisation had a "*painless resolution*" and the account was resecured. The next stage involved educating the MD not to enter his password into a site unless he knew what it was for. The MD was receptive to this action.

This support journey demonstrates the importance for SMEs of building a strong and trusting working relationship with an MSP who understands the organisation. The MSP's existing knowledge was an advantage in resolving the issue effectively and efficiently.

4.5 Support Journey E - Access Management

The IT manager of a property service organisation described an issue with multi-factor authentication (MFA) prompts. No change control had been applied, meaning prompts were sent for every interaction with Office 365 and became disruptive. The MSP paused the change due to the impact and implemented user acceptance testing, which had been recommended by the SME. Although prompts then triggered in the appropriate timeframe, this did not happen consistently or across all applications. The SME therefore decided not to roll out MFA with the existing provider and requested architectural support to redesign the MFA process.

In a follow-up instance, the IT manager described that the user testing pilot group had not authenticated across all accounts and had not triggered when logging on from a new location, such as WiFi. Six months after the initial issue, the MFA configuration still required review. As the IT manager described, "*testing is key to understand what happens and then be able to communicate to users. The reasons for a change need to be well communicated*". The SME also expressed frustration that the provider was not proactive in seeking continuous improvements.

4.6 Support Journey F - Cyber Essentials Certification

Cyber Essentials is a UK government-backed certification programme that helps keep organisations' and customers' data safe from cyber attacks [22]. In this support journey, the co-owner of a mental health charity with approximately 11 employees wanted to be recertified and had the opportunity for this to be sponsored. After registering for certification and sending details to the sponsoring organisation for payment, she received access to the IASME portal.

She described the IASME team as "*very patient with me as I didn't understand exactly what the questions were asking for. However, once they explained these to me it was a lot clearer*". She also explained that "*it was a case of working out what was expected with the terminology being used before being able to supply a response*", adding that "*the IASME support team were brilliant*".

Although the participant described IASME support positively, she also needed to develop her own workaround by copying responses into a Word document alongside

the portal to ensure answers were retained. This suggests that, even where interpersonal support is positive, the practical process of completing certification may still require additional effort and confidence from SMEs. For some organisations, this friction could affect completion, especially where cyber security terminology and online submission processes are unfamiliar.

4.7 Support Journey G – Risk Management

Cyber security providers may receive contact from SMEs looking for advice about how to improve cyber security without knowing what the solution should be. In this support journey, an SME was referred to a cyber security provider "*enquiring about cost effective methods to reduce cyber risk to their business*". The SME was taking a proactive approach to risk management but did not know how to proceed.

After several conversations, the provider recommended Cyber Essentials as an appropriate solution. The SME was not originally aware of how Cyber Essentials could benefit them, so a major part of the journey involved explaining how it would meet their needs and how they could benefit from certification. The SME later "*achieved certification and implemented steps to protect their business*". The provider did not report many challenges, partly because the SME was "*engaged and wanted to improve their security there*".

This support journey demonstrates the importance of cyber security providers spending time to understand the SME, its context, and its current cyber security posture. It also shows that successful support may be more likely when the SME is motivated to improve its cyber security.

4.8 Support Journey H - Phishing Incident

One provider described responding to a phishing incident involving one of their customers. The provider reported that their "*customer's email had sent out hundreds of phishing emails to their clients*". On investigation, engineers discovered that the customer had clicked on a phishing link, giving the attacker full access to the email account because MFA had been switched off.

Although the provider resolved the issue, they found it "*frustrating that the basics of security were not employed and that no alert was incoming to us of the fact it had been taken off. This would have prevented the attack*". The provider advised the customer to contact their clients and the Information Commissioner's Office (ICO). The provider also noted that the customer's client denied clicking on the link, which delayed identifying the issue. They expressed frustration that customers were not "*getting some of the fundamentals*" and argued that MFA should be mandated, with an alert mechanism when a 365 tenant has MFA switched off.

This support journey shows that cyber security providers and SMEs need to work in partnership to achieve effective cyber security. Although the provider was frustrated with the SME for not "*getting some of the fundamentals*", there was little evidence of developing the SME's knowledge beyond the commissioned monitoring of phishing

emails. The outcome reinforces that providers should not assume SMEs always know the right action to take or how to effectively support their own clients.

Table 2. Summary of the eight support journeys presented in the paper

Journey	Topic	Source of journey	Support route	Trigger	Outcome
A	SSL Certification	SME (Sole Trader, Health and Social Care)	Hosting provider / online support	Expired SSL certificate identified by a customer.	Issue eventually resolved, but with dissatisfaction, delays, and concern about future renewal.
B	Incident Preparedness	SME (20 employees, Information and Communication)	NCSC guidance and internal discussion	NCSC newsletter and British Library cyber attack review prompted reflection.	Improved awareness and internal discussion about incident communication and preparedness.
C	Data Protection	SME (20 employees, Information and Communication)	External provider search	Business continuity concerns and follow-up provider proposals.	Search paused because proposed support did not align well with the SME's needs or timing expectations.
D	Incident Response	SME (200 employees, Transport and Storage)	Existing MSP relationship	Suspected incident involving fraudulent bank detail communication.	Rapid and effective resolution through a trusted MSP with existing organisational knowledge.
E	Access Management	SME (63 employees, Property and Real Estate)	Existing provider / architectural support	Problems with MFA prompts and change control.	Further review and redesign required after inconsistent implementation and user testing issues.
F	Cyber Essentials Certification	SME (11 employees, Health and Social Care)	IASME / certification portal support	Need for Cyber Essentials recertification.	Support experience was positive overall, but portal design created frustration and risk of lost work.
G	Risk Management	Cyber security advisory provider	Provider-led	SME sought cost-effective ways to	Provider recommended Cyber Essentials and the

Journey	Topic	Source of journey	Support route	Trigger	Outcome
			advisory route	reduce cyber risk.	SME achieved certification.
H	Phishing Incident	Cyber securit incident response provider	Provider incident response	Customer phishing incident after MFA had been switched off.	Incident resolved, but exposed weak cyber hygiene and the need for stronger preventive measures.

4.9 Summary of Results

Comparison across the eight selected cases revealed recurring patterns in how support was accessed, delivered and experienced. Each support journey dealt with a different cyber security issue and organisational context, but comparison across the eight cases revealed recurring patterns in how support was accessed, delivered and experienced . There appeared to be three broad factors underpinning more effective support journeys: an understanding of the SME's context; transparency in interactions; and provider proactivity.

Understanding the SME context. Support was more effective across multiple journeys when providers understood the SME's operational environment, existing arrangements, cyber security knowledge and practical constraints. This was demonstrated in the Incident Response journey where the current MSP's knowledge of the organisation allowed for an efficient and appropriate response. The provider also re- recommended Cyber Essentials after understanding the SMEs needs in the Risk Management journey. Conversely, the Data Protection journey revealed how frustration could occur when support was not entirely aligned with the SME's infrastructure, priorities or expectations. Providers should avoid assumptions and start support journeys with clear two way communication around the problem, the current position of the SME and the constraints around which support needs to be delivered.

Transparency in interactions. A second common theme was the need for clear, transparent communication. Support was seen more favourably when expectations, terminology, responsibilities and next steps were clearly explained and less favourably when communication was incomplete or ambiguous. The SME liked the way IASME explained what was being asked and clarified terminology on the Cyber Essentials Certification journey. On the other hand, the SSL Certificate journey indicated dissatisfaction in the lack of clear communication of essential information such as expiry of the certificate and availability of support. Similar issues were noted on the Data Protection and Access Management journeys, where the experience could have been improved with more explicit explanation of the scope, rationale and limitations of support. Practical recommendations therefore include explaining what needs to be done, when sup-

port is available, likely costs or limitations, and what the SME should expect at each stage.

Provider proactivity. The third factor concerned the extent to which providers or support sources took an active role in guiding the SME. Support was more successful when providers anticipated issues, prompted action, followed up, or helped move the SME toward a workable solution. This was evident in the Incident Preparedness journey where the NCSC newsletter was a proactive prompt and in the Incident Response journey where the MSP led the investigation and corrective action, resulting in a "painless resolution". In contrast, the SSL Certificate, Data Protection, Access Management and Phishing Incident journeys showed missed opportunities for earlier warning, stronger guidance, testing or preventative action. The proactive support was particularly valuable, not just because it resolved the immediate issue but also because the SME came away better informed and more confident. Overall, these findings suggest that effective cyber security support for SMEs is dependent not only on technical expertise but also on understanding the organisation, clear communication and active guidance of the support process. These factors may be particularly important for SMEs, which often have fewer internal cyber security resources and rely on external providers to translate technical advice into practical action.

5 Discussion

This study examined how SMEs seek and experience cyber security support in practice. Comparative analysis of the eight selected journeys identified three broad clusters that appeared to shape support experiences: i) understanding the context of the SME, ii) transparency in interactions, and iii) proactivity of the provider.

5.1 Understanding the context of the SME

A recurring pattern across the support journeys was the importance of understanding the organisational context within which the SME operates. Support appeared most effective when providers tailored their advice to the SME's systems, resources, responsibilities, and level of cyber security knowledge. This aligns with previous research showing that SMEs may struggle to manage IT resources and interpret cyber security controls without context specific support [14, 23]. It also aligns with evidence that SME cyber security practices vary across organisational characteristics, reinforcing the need for support that is tailored rather than generic [24].

The current findings add to this literature by showing how contextual understanding shapes the support journey itself. In the Incident Response journey, the MSP's existing relationship with the organisation meant that it already understood the SME's infrastructure and was able to respond quickly to the potential incident. In contrast, in the Data Protection journey, frustration arose where proposed support did not fully align with the SME's existing arrangements, expectations, or timing needs. This implies that effective support is not only about making technically sound recommendations but

about ensuring that those recommendations are workable in the specific operational environment of the SME.

A more explicit diagnostic stage could therefore be built into provider interactions for future support for SMEs. Providers could assess the SME's existing systems, internal responsibilities, level of cyber security awareness, time constraints and preferred ways of working before recommending solutions. This can help to prevent mismatches between the support offered and the support required, and enable providers to tailor advice in a way that can be realistically applied by SMEs.

5.2 Transparency in interactions

A second important factor concerned transparency in interactions between SMEs and providers. Support was viewed more positively when providers explained terminology, clarified expectations, and made next steps understandable. This aligns with research showing that cyber security advice can be difficult for non-experts to prioritise and act upon [13], and with work highlighting uncertainty in cyber security decision-making among small-scale organisations and users [3, 20].

The current findings show that transparency matters not only in written guidance, but also in provider-SME interactions. In the Cyber Essentials Certification journey, the participant's positive experience was shaped by the support team's willingness to explain terminology and clarify what was being asked. In contrast, the SSL Certificate journey illustrated how uncertainty about the problem, the renewal process, and the availability of support contributed to dissatisfaction. Similar communication challenges were visible in the Data Protection and Access Management journeys, where clearer explanations of the proposed changes, limitations, and expected outcomes may have improved the support experience.

Future SME support could therefore be improved by making communication more explicit and structured. Providers could set out what the issue is, why it matters, what action is required, who is responsible for each step, what the likely timescale is, and what the SME should expect next. Written summaries after support interactions may also be useful, particularly for SMEs without internal cyber security expertise. In this way, transparency is not only about being clear, but about reducing uncertainty and enabling SMEs to act with greater confidence.

5.3 Proactivity of the provider

The third factor influencing effective support journeys was whether providers adopted a proactive rather than purely reactive approach. Support appeared more effective when providers helped SMEs anticipate risks, understand implications, and take appropriate next steps. This aligns with research showing that SMEs face barriers to cyber security risk management [5], that risk perceptions shape precautionary security behaviour [6], and that SMEs often face resource, awareness, and implementation constraints [8, 18]. This also aligns with recent work showing that SME cyber security awareness support is most effective when it is context-specific, practical, and reinforced over time [25].

The support journeys add detail to this issue by showing how provider proactivity can shape whether support becomes merely corrective or also preventative. In the Incident Response journey, the MSP took the lead in investigating the issue and re-securing the account, resulting in a rapid resolution. In the Incident Preparedness journey, the NCSC newsletter acted as a proactive prompt that encouraged the SME to reflect on incident communication and preparedness before an incident occurred. By contrast, the SSL Certificate, Access Management, Data Protection, and Phishing Incident journeys all suggested missed opportunities for earlier warning, clearer follow-up, better testing, or stronger preventative measures.

Future support for SMEs could therefore place greater emphasis on proactive guidance rather than reactive problem-solving alone. Providers could use support interactions as opportunities to identify related vulnerabilities, explain preventative controls, and agree follow-up actions. For example, resolving an incident could be paired with a short review of what made the incident possible, what controls could reduce recurrence, and what the SME should monitor in future. This would help shift support from isolated problem resolution towards capability-building, where SMEs are left better equipped to recognise and manage similar issues in the future.

5.4 Implications

This work sheds light on some of the ways in which SMEs can receive effective cyber security support, either from a cyber security provider or with no provider interaction. By analysing eight support journey cases from a variety of areas within cyber security we were able to identify a number of effective strategies for support. The implications of these findings for various stakeholders are discussed below.

Firstly, for technical authorities such as the NCSC and policymakers, these findings may help inform providers in how best to support SMEs. From the findings within the current study, the findings suggest there are frustrations that SMEs may have when working with providers, some of which might be overcome if providers are made aware of how to support SMEs. This also aligns with wider research on SME digital capability which highlights the importance of targeted and flexible training support to help SME decision-makers understand and apply technical concepts in practice [15].

Secondly, for cyber security providers, there are practical implications for how to work effectively with SMEs, beyond having technical knowledge in the field. Many providers may feel that having sufficient knowledge in cyber security is sufficient to achieve the required support for the SME, when there is a clear need to adopt skills that may be more 'soft' in nature to achieve a positive outcome.

Thirdly, for SMEs, SMEs may benefit from being aware of some of the pitfalls that may arise when working with a cyber security provider. Evaluating potential providers on criteria that align with the findings within the current study may help to identify providers that are a good fit for the SME. It may also be necessary for the SME to do greater due diligence on a potential provider, such as seeking references on not only what they can provide, but how they provide cyber security support.

5.5 Strengths and Limitations

This study is among the first to examine cyber security support as a support journey unfolding over time, capturing how SMEs and providers interact across multiple stages of support. The current research gives rise to a number of ways in which cyber security providers can approach their work with SMEs in an effective manner. The findings provide technical authorities such as the NCSC with evidence that can support the development of practical guidance for providers working with SMEs.

A further strength of the study is that it captured support journey instances close to the point at which they occurred and included perspectives from both SMEs and cyber security providers, enabling insight into support experiences as they unfolded rather than relying solely on retrospective recall.

The support journeys presented in this paper were purposively selected from the wider dataset on the basis that they contained the most detailed and complete accounts of support interactions. Accordingly, the findings should be interpreted as illustrative rather than representative of all possible SME cyber security support journeys.

A further limitation concerns participant engagement. Although 21 SMEs and 24 providers were recruited, submitted instances were received from only 12 SMEs and 14 providers. As each participant took part for a rolling three-month period, some may not have experienced a relevant support journey during that window. Others may have lacked time, confidence, or willingness to document cyber security issues, particularly where interactions were sensitive, minor, or commercially confidential. As a result, the dataset may be affected by participant engagement and response bias, and is likely to reflect the journeys participants noticed, prioritised, and were able to report, rather than the full range of support interactions that occurred.

6 Conclusions

SMEs rely on different forms of support to strengthen their cyber security resilience, whether through direct engagement with cyber security providers or through other sources such as online guidance and resources. This study set out to examine what happens when SMEs seek support for a cyber security question or concern, and how those support experiences unfold in practice.

Through comparative analysis of eight support journey cases, the study suggested that effective cyber security support depends not only on technical expertise, but also on how support is delivered and experienced by SMEs. Across the cases, three recurring factors were identified as central to effective support journeys: understanding the context of the SME, transparency in interactions, and proactivity of the provider. Support appeared to be more effective when providers took time to understand the SME's specific circumstances, communicated clearly about problems, processes, and expectations, and adopted an active role in guiding the SME through the support process. Ineffective support journeys were often characterised by misalignment between support offered and actual needs, unclear communication, and missed opportunities for proactive guidance. This reinforces that advice must be accessible, relevant, and workable within the SME's operational context.

Overall, this paper contributes exploratory insight into how SME cyber security support journeys are experienced in practice and offers practical considerations for improving them. For providers, the findings emphasise the importance of tailoring support, communicating transparently, and helping SMEs build their understanding over time. For SMEs, the findings highlight the value of seeking providers and support routes that are responsive, clear, and able to engage with their specific organisational needs. Taken together, the results suggest that improving cyber security support for SMEs requires greater attention not only to what support is provided, but also to how that support relationship is structured and sustained. Future work should examine a larger and broader set of journeys, including follow-up interviews to validate whether these exploratory patterns hold across wider SME support experiences.

Acknowledgments. This study was 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: Cyber security breaches survey 2025. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025, last accessed 2026/03/03 (2025)
2. Kaila, U., Nyman, L.: Information security best practices: First steps for startups and SMEs. Technology Innovation Management Review 8(11), 32–42 (2018)
3. Renaud, K., Weir, G.R.: Cybersecurity and the unbearability of uncertainty. In: Cybersecurity and Cyberforensics Conference (CCC), pp. 137–143. IEEE (2016)
4. Papathanasiou, A., Liontos, G., Katsouras, A., Liagkou, V., Glavas, E.: Cybersecurity guide for SMEs: Protecting small and medium-sized enterprises in the digital era. Journal of Information Security 16(1), 1–43 (2025)
5. Alahmari, A., Duncan, R.A.: Investigating potential barriers to cybersecurity risk management investment in SMEs. In: 2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), pp. 1–6. IEEE (2021)
6. Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., Kusev, P.: Risk perceptions of cyber-security and precautionary behaviour. Computers in Human Behavior 75, 547–559 (2017)
7. Bada, M., Sasse, M.A., Nurse, J.R.C.: Cyber security awareness campaigns: Why do they fail to change behaviour? In: International Conference on Cyber Security for Sustainable Society, pp. 118–131 (2015)
8. Adriko, R., Nurse, J.R.C.: Cybersecurity, cyber insurance and small-to-medium-sized enterprises: A systematic review. Information and Computer Security 32(5), 691–710 (2024)
9. Alahmari, A., Duncan, B.: 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 (2020)

10. Chaudhary, S., Gkioulos, V., Katsikas, S.: A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. Computer Science Review 50, 100592 (2023)
11. National Cyber Security Centre: Small business guide. https://www.ncsc.gov.uk/collection/small-business-guide, last accessed 2026/03/03 (2020)
12. Khan, N., Furnell, S., Bada, M., Nurse, J.R.C., Rand, M.: Assessing cyber security support for small and medium-sized enterprises. In: International Symposium on Human Aspects of Information Security and Assurance, pp. 148–162. Springer (2024)
13. Redmiles, E.M., Warford, N., Jayanti, A., Koneru, A., Kross, S., Morales, M., Stevens, R., Mazurek, M.L.: A comprehensive quality evaluation of security and privacy advice on the web. In: 29th USENIX Security Symposium (USENIX Security 20), pp. 89–108 (2020)
14. Cragg, P., Mills, A., Suraweera, T.: Understanding IT management in SMEs. Electronic Journal of Information Systems Evaluation 13(1), 27–34 (2010)
15. Azevedo, A., Almeida, A.H.: Grasp the challenge of digital transition in SMEs—A training course geared towards decision-makers. Education Sciences 11, 151 (2021)
16. Hoong, Y., Rezania, D., Baker, R.: When traditional SME managers encounter cybersecurity: Discourse analysis of opportunities and dilemmas in meeting the demands. Technology in Society 78, 102650 (2024)
17. Hoong, Y., Rezania, D.: Balancing talent and technology: Navigating cybersecurity and privacy in SMEs. Telematics and Informatics Reports 15, 100151 (2024)
18. Benjamin, L.B., Adegbola, A.E., Amajuoyi, P., Adegbola, M.D., Adeusi, K.B.: Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies. Global Journal of Engineering and Technology Advances 19(2), 134–153 (2024)
19. Hoppe, F., Gatzert, N., Gruner, P.: Cyber risk management in SMEs: Insights from industry surveys. Journal of Risk Finance 22(3–4), 240–260 (2021)
20. Osborn, E., Simpson, A.: Risk and the small-scale cyber security decision making dialogue - A UK case study. Computer Journal 61(4), 472–495 (2017)
21. Yin, R.K.: Case Study Research and Applications: Design and Methods. 6th edn. Sage, Thousand Oaks (2018)
22. National Cyber Security Centre: Cyber essentials overview. https://www.ncsc.gov.uk/cyber-essentials/overview, last accessed 2026/03/03
23. Renaud, K., Ophoff, J.: A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. Organizational Cybersecurity Journal: Practice, Process and People 1(1), 24–46 (2021)
24. Rand, M., Bada, M., Khan, N., Furnell, S., Nurse, J.R.C.: Understanding cyber security practices in SMEs: A mixed-methods investigation. Information Security Journal: A Global Perspective, 1–39 (2026)
25. Ugbebor, F., Aina, O., Abass, M., Kushanu, D.: Employee cybersecurity awareness training programs customized for SME contexts to reduce human-error related security incidents. Journal of Knowledge Learning and Science Technology 3(3), 382–409 (2024)