Rand, Matthew, Bada, Maria, Furnell, Steven, Nurse, Jason R. C. and Khan, Neeshe (2026) *Understanding cyber security practices in SMEs: A mixed-methods investigation.* Information Security Journal: A Global Perspective . ISSN 1939-3555.

INFORMATION SECURITY JOURNAL: A GLOBAL PERSPECTIVE
https://doi.org/10.1080/19393555.2026.2648174

Taylor & Francis
Taylor & Francis Group

OPEN ACCESS Check for updates

Understanding cyber security practices in SMEs: A mixed-methods Investigation

Matthew Rand[a], Maria Bada[a], Steven Furnell[b], Jason R.C. Nurse[c], and Neeshe Khan[b]

[a]School of Biological and Behavioural Sciences, Queen Mary University of London, London, UK; [b]School of Computer Science, University of Nottingham, Nottingham, UK; [c]School of Computing, University of Kent, Canterbury, UK

ABSTRACT

Small and medium-sized enterprises (SMEs) encounter cyber security risks, yet the factors underlying variation in these risks remain unclear. This study examined whether 1) cyber security controls, 2) awareness, knowledge, attitude, culture and 3) support routes vary according to SME characteristics (size, type, maturity and sector). It also explored the factors that shape SMEs' decisions to access resources that help reduce cyber security risk. A mixed-methods design combined a survey of 374 participants and interviews with 12 SMEs. ANOVAs analyzed differences across organizational categories, and thematic analysis was applied to qualitative data. The study shows that many SMEs in the sample have inadequate security controls and limited awareness, knowledge and capability in cyber security. Qualitative insights show that SMEs may underestimate risk, face competing priorities and are unsure where to find support. These findings highlight the need for practical, accessible support to help SMEs implement effective cyber security.

KEYWORDS

Cyber hygiene; cyber security; cyber security behaviour; cyber security support; SMEs

1. Introduction

A significant proportion of both employment and turnover in developed countries is accounted for by small and medium-sized enterprises (SMEs) (OECD, 2023). Within the UK as a specific example relevant to this paper, The Federation of Small Businesses (FSB) estimates that as of 2024, there were approximately 5.5 million SMEs within the UK, accounting for approximately half of all revenue in the UK private sector (FSB, 2024). Despite there often being a misconception that cyber threats primarily concern larger organizations, SMEs (i.e. those organizations with fewer than 250 employees) are continually facing similar threats too (Manzoor et al., 2024). Approximately 50% of small organizations and 67% of medium organizations report that they have observed breaches or attacks within their organizations in the previous 12 months, with Phishing, Impersonation and Malware the most commonly identified types of incidents (DSIT, 2025). Whilst these statistics may feel somewhat alarming, the true number of cyber incidents in SMEs may well be even higher given that SMEs often do not report cyber security incidents (Ikuero & Zeng, 2022). Understanding how SMEs can increase their cyber resilience is therefore key.

One potential reason for the relatively high number of cyber security incidents in SMEs is their increasing use of online technology, where existing business models have been adapted with the continual opportunities and transformation that new technologies provide (Jafari-Sadeghi et al., 2021). Whilst these uses of technology have many organizational benefits, it has created a growing attack surface as a result of many SMEs moving toward high usage of the internet and the cloud (Pawar & Palivela, 2023). Thus, this changing dynamic has generated new challenges in organization designs, management systems and information security risks for SMEs (Soomro et al., 2016). SMEs also often act as third parties to larger organizations in the form of contractors and vendors and cyber attackers may use SMEs as a mechanism to access the systems of larger organizations (Verizon, 2024). Given the increasing use of technology and their close collaboration with larger organizations through respective supply chains, the need to focus on SMEs as well as larger organizations is therefore warranted (Hoppe et al., 2021). SMEs also arguably need to have cyber defenses that are on the same level as large organizations if they are to remain secure from cyber security threats.

CONTACT Matthew Rand m.rand@qmul.ac.uk QMUL School of School of Biological and Behavioural Sciences, Mile End Rd, London, E1 4DQ, UK

In addition to the growing usage of internet technologies, a larger process of digitization and digital transformation happening in SMEs is also very important to consider. Digitization can be described as the use of digital technology in corporate processes and operating models, including using cloud services and connected digital infrastructures (Metin et al., 2024; Saeed et al., 2023). Whilst digitization can enhance efficiency, flexibility and competitiveness, it may also increase organizational exposure to cyber threats, given that greater connectivity and data exchange can introduce additional vulnerabilities and entry points for attack (M. F. Arroyabe, C. F. A. Arranz, J. C. Fernandez de Arroyabe, et al., 2024; Saeed et al., 2023).

Recent syntheses of the literature have noted that digitization and cyber security are often examined separately, despite clear interdependencies between digital transformation and cyber risk exposure in SMEs (M. F. Arroyabe, C. F. A. Arranz, J. C. Fernandez de Arroyabe, et al., 2024). In this context, cyber resilience can be viewed not only as a protective function but as a necessary condition for sustaining digital adoption and organizational continuity (Metin et al., 2024). It is therefore becoming more important to understand how SMEs put controls in place, increase their awareness and ask for support when digitalization is increasing and exposure to cyber threats may be structurally embedded within their organizational operations (Saeed et al., 2023).

Although all organizations with fewer than 250 employees are categorized as an SME within the UK, organizations categorized as an SME are heterogenous in their make-up (e.g. size and type) and their cyber security needs (Shojaifar & Järvinen, 2021). To date, whilst there has been a wealth of research exploring various factors such as the awareness, knowledge, attitudinal and cultural levels of cyber security within SMEs to understand their cyber security effectiveness, there has been a paucity of research that has explained the potential reasons for these levels. It could be that this heterogeneity plays a key role and that not all SMEs are the same in these areas, which this study will aim to explore further. This study therefore aims to examine whether 1) cyber security controls, 2) awareness, knowledge, attitude, culture and 3) support routes vary based on organizational category. The current study also seeks to understand the types of support that SMEs would benefit from to reduce their cyber security risk. The value of the current study is therefore evident in two broad areas: firstly, it will go beyond previous studies that have established that SMEs generally have low levels of awareness, knowledge, attitude and cultural levels toward cyber security. As SMEs are heterogeneous in nature, it is not clear whether all SMEs have similar levels within these areas or whether their heterogeneity could explain how SMEs are approaching cyber security (e.g. does an element of heterogeneity, such as organizational size, explain higher or lower levels). This study takes a quantitative approach through the analysis of a survey instrument on SMEs to understand this first area. The qualitative strand complements this by exploring in greater depth how SMEs interpret and act on cyber security support in practice. Together, these mixed methods provide both a broad and contextual understanding of the factors that influence SME cyber security behavior and the support needed to improve resilience.

2. Related works

2.1. Employee awareness and knowledge

From a human factors perspective, increasing awareness of employees has often been seen to be an indispensable aspect of organizations' cyber security strategy to reduce the potential negative consequences of cyber threats (Chaudhary et al., 2023; Li et al., 2022; McCormac et al., 2017). This is despite awareness raising activities and programmes previously being cited as not sufficient to provide the necessary outcomes to reduce this risk (e.g., Bada et al., 2015; Stewart & Lacey, 2012). For example, in one study, despite many employees displaying sufficient knowledge within awareness campaigns and training courses about how to act in a cyber secure manner, only 64% of their behavioral intentions translated to desirable action (Gundu, 2019). Raising awareness and knowledge is therefore necessary but not achievable on its own to change behavior, as evidenced by various behavior change models, for example the COM-B, which identifies *Opportunity* and *Motivation* as fundamental for behavior change alongside *Capability* (i.e. awareness and knowledge) (Michie et al., 2014). Despite this, a growing literature base has suggested that SMEs tend to lack awareness of the cyber security threats they may face (e.g., Bada & Nurse, 2019; Saban et al., 2021). Meanwhile, some research has concluded that it is only the technology departments and leadership teams that have awareness of cyber security (Huaman et al., 2021). On the contrary some research has concluded that employees actually have the awareness of potential threats and it is the SMEs leadership team that has lacked the required awareness, resulting in the deprioritisation of cyber security (e.g., Ahmed & Nanath, 2021; Ključnikov et al., 2019). Interestingly, there is also a body of research that has indicated that it is specifically limited knowledge and also an understanding of cyber security risk, instead of awareness, which is leading to poor cyber security in some SMEs (Adriko & Nurse, 2024; Carias et al., 2020; Obreja et al., 2025), with this lack of knowledge particularly attributable to SME leaders (Barlette & Jaouen, 2019; Barlette et al., 2017). Thus, whilst there is a growing literature base to suggest that SMEs have a generally low cyber security awareness, this view is not conclusive, as some research has suggested that certain employees within SMEs may have awareness and it could be specific employees within the organization that lack it (such as leadership).

2.2. Attitude toward cyber security

Given that awareness and knowledge of cyber security are unlikely to translate to behavior on their own, they require additional factors such as attitude and commitment to protect the organization. Even if employees display the required awareness and knowledge, their attitudes and commitment are fundamental in influencing behavior to build cyber resilience (Kaur & Mustafa, 2013). Employees with an increased cyber security knowledge and an increasing positivity toward cyber security are more likely to engage in compliant behavior toward cyber threats (Alshaikh et al., 2021). Earlier research by Lee and Larsen (2009) similarly emphasized that cyber security adoption decisions within SMEs are influenced by perceptions of threat and coping ability. They found that how people feel about vulnerability and how effective they think their responses are strongly affects how organizations prioritize and spend money on protective measures. Along with awareness, knowledge and attitude, how SMEs perceive cyber security risk may explain how they behave toward the risk. Studies have reported that SMEs may underestimate their vulnerability to general cyber security risks, even though they might be aware of the potential risks (Barlette et al., 2017; Van Schaik et al., 2017; Wilson et al., 2023). Displaying overconfidence in their recognition and evaluation of cyber security risks may be a factor in how SME employees perceive risk (Alahmari & Duncan, 2021). In a study of 20 decision makers from SMEs, many respondents did not identify cyber security as a threat, had not knowingly been a victim of a cyber-attack and had overconfidence in their technology business partners (Alahmari & Duncan, 2021). These aspects might make it hard for them to see the possible cyber security risks they could face. SMEs might not pay attention to cyber security risks because they think they are not big or important enough to be attacked by hackers (Mitrofan et al., 2020; Saban et al., 2021). Thus, SMEs may have the belief that their cyber defenses are adequate because of this perception that attackers are primarily targeting larger organizations. SMEs may also not see many benefits of cyber defenses (Rae & Patel, 2019, 2020), underestimate the value of their assets (Ulrich et al., 2020) and believe they have fewer cyber security risks (Rae & Patel, 2020). All of these factors may explain why SMEs tend to not pay the attention that is needed toward cyber security risks.

2.3. Organizational culture

Strong cyber security risk management decision making in SMEs is also reliant on owners and senior managers (Barlette et al., 2017) who are likely to be influencing the cyber security culture of the SME (Uchendu et al., 2021). Such security decisions may not only affect their own organization but many organizations and industries, and could have a considerable impact on the supply chain's wider security (Osborn & Simpson, 2018). Whilst SMEs senior managers are directly involved in cyber security decisions, these senior managers also regularly utilize experts and social networks to support these decisions (Barlette et al., 2017). Therefore, senior managers, in addition to experts and professionals, could significantly influence the SMEs decision making process toward cyber security and creating a strong cyber security culture. Implementing a security culture within an SME can have a series of challenges when compared to large organizations (Gerst et al., 2024). For example, a lack of money, knowledge and time needed to implement cyber security in an efficient manner may act as barriers to a strong cyber security culture (Santos-Olmo et al., 2016). SMEs may also not have procedural policies in place that larger organizations have or define the responsibilities of their users, with employees needing to be aware of their role in preventing and reducing cyber security threats and must be committed to staying up to date with current policies and procedures to mitigate and respond to security threats (Saban et al., 2021).

2.4. Implementing controls

SMEs generally express concerns about cyber security, yet only a small number understand 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 (Renaud & Ophoff, 2021). A lack of situational awareness of which resources are the most helpful and relevant may also hinder rather than help SMEs on what potential actions to take (Renaud & Ophoff, 2021). There has been minimal research investigating which cyber security controls have been adopted by SMEs, with recent empirical studies indicating that SMEs lack fundamental cyber security measures and frequently lack frameworks to facilitate implementation (Pawar & Palivela, 2022). Heidt et al. (2019) similarly concluded that smaller organizations often do not have the same structured management processes, technical safeguards, and resources that larger organizations do. This gap shows that SMEs require ways that are tailored for them, not scaled down versions of frameworks that are designed for larger organizations. SMEs may also encounter challenges in financing cyber security, implementing appropriate measures, or recruiting individuals with the requisite expertise (Osborn & Simpson, 2017; Pawar & Palivela, 2023). There is also proof that smaller organizations are less likely to have explicit rules and procedures in place to keep themselves safe from cyber threats (DSIT, 2025).

SMEs can take a number of simple but effective steps to avoid a cyber security issue. For example, they can set minimum password requirements, install security patches on time, use multi-factor authentication, and set up an automatic backup system (Kaila & Nyman, 2018).

2.5. Organizational maturity

Maturity models are commonly used to describe how organizational practices develop over time, typically progressing from informal and reactive activity toward more established and systematically managed routines. Staged approaches such as the Capability Maturity Model conceptualize progression across identifiable levels, where later stages are characterized by clearer processes, greater repeatability, and more structured monitoring and improvement (Becker et al., 2009; Paulk et al., 1993). In CMMI-style approaches, organizations are understood to evolve through defined levels of capability, moving from ad hoc practices toward increasingly standardized, measured, and continuously improved processes. Although originally developed in software contexts, the underlying logic has been applied more broadly to organizational capability development (CMMI Product Team [CMMI], 2018).

Governance focused maturity approaches, including those associated with ISACA and COBIT, similarly frame maturity in terms of increasing formalized and documented policies and control structures (De Haes & Van Grembergen, 2009). Studies of cyber security maturity models highlight variation in how maturity is defined and assessed, reflecting the diversity of available models and standards (Rabii et al., 2020; Yigit Ozkan & Spruit, 2022). At the same time, many frameworks adopt a staged logic in which organizations progress from informal or reactive approaches toward more rigorous and risk-informed security practices and controls (Yigit Ozkan & Spruit, 2022). Across these perspectives, maturity is therefore understood not simply as organizational age, but as the degree to which structures, routines, and management practices have become established over time.

Developmental stage in organizations can be associated with shifts from informal, founder-centric management toward more structured coordination, clearer role definition, and increased process formalization (Levie & Lichtenstein, 2010; Phelps et al., 2007). As organizations grow, managerial roles tend to become more differentiated, decision-making processes more formalized, and internal systems more clearly articulated. In smaller and younger organizations, routines may be emergent, experience-based, and undocumented, whereas more developed organizations are more likely to exhibit greater institutionalization of procedures, clearer accountability mechanisms, and more explicit governance arrangements (Davila et al., 2010). In this sense, organizational developmental stage provides a practical lens for capturing variation in how structures, routines, and management practices are embedded within SMEs.

In the present study, organizational maturity is treated as an organizational developmental stage. It reflects whether an SME is in an early stage of formation, in growth, established, mature, or positioned as an industry leader. In this context, maturity is an indicator of organizational development used to examine whether the provision of cyber security differs across stages of SME development.

2.6. Digitization

Digitization has become an increasingly prominent feature of SME development. It is commonly defined as the integration of digital technologies into organizational processes, products, and services, often involving the use of cloud computing and interconnected systems (Metin et al., 2024; Saeed et al., 2023). Within SME contexts, digitization is frequently associated with enhanced competitiveness, improved operational efficiency and opportunities for innovation, although it may also present practical challenges relating to skills, cost, and implementation capability (Goh & Singh, 2023).

Alongside these benefits, digitization has implications for cyber security risk. Increased connectivity, reliance on digital infrastructures and expanded data processing can introduce additional vulnerabilities and broaden the potential attack surface of SMEs (M. F. Arroyabe, C. F. A. Arranz, J. C. Fernandez de Arroyabe, et al., 2024; Saeed et al., 2023). Evidence synthesizing research on SMEs suggests that digital transformation is associated with heightened cyber exposure and the need for appropriate mitigating controls and standards to reduce vulnerabilities (M. F. Arroyabe, C. F. A. Arranz, J. C. Fernandez de Arroyabe, et al., 2024). Emerging operational frameworks further emphasize that cyber security should not be considered in isolation from digital transformation, but rather as embedded within governance structures, organizational culture and continuous improvement processes (Metin et al., 2024). From this perspective, the development of cyber security capability can be understood as part of enabling secure digitization over time (Saeed et al., 2023).

Despite this, SMEs may face barriers in translating available guidance into practice, including uncertainty about which resources are relevant and difficulty navigating competing advice (Renaud & Ophoff, 2021). Digitisation may therefore increase both opportunity and exposure, reinforcing the importance of examining how SME characteristics relate to the implementation of specific cyber security controls, levels of awareness, knowledge, attitude, and culture.

2.7. Seeking support

Awareness of the Cyber Essentials Scheme (NCSC, 2020) is lowest amongst small businesses with only a small proportion adhering to the scheme (DSIT, 2025), despite government sponsored schemes previously enabling small businesses to have grants to pay for such accreditations (Renaud & Ophoff, 2021). Thus, it is clear that the responsibility is on the SME to seek out and follow the advice that will help them to prevent cyber attacks affecting their organization. However, the materials available to SMEs vary considerably, which could cause them to be confused about which resources are most appropriate for them and thus hinder their decision making (Khan et al., 2025). What is less clear is whether SMEs are seeking out alternative sources of guidance to support them and if not, the factors that may explain this behavior. There may be barriers to cyber security investment such as lack of awareness, financial capacity or overconfidence of decision-makers (Alahmari & Duncan, 2021).

A way that awareness training may change behavior is through shifting employee attitudes toward cyber security. In one study, cyber awareness training was important in affecting threat appraisal (i.e. employees' perception toward threat severity and perception toward threat vulnerability) (Wong et al., 2022). Educating employees to understand potential forms of cyber attacks can potentially not only help employees to avoid falling for cyber security threats, but may support them in assessing how severe the threat is and understand the employees' own vulnerabilities (Wong et al., 2022). These findings align with earlier research that threat and coping appraisals, particularly perceptions of severity, vulnerability, and response efficacy, drive protective adoption behavior in SMEs (Lee & Larsen, 2009). Given the importance of cyber security awareness training for SME employees, it is imperative to understand which types of support work best for employees and in which contexts. As SMEs are unlikely to have the resource to provide in house provision, they will need to seek awareness training from outside the organization for their employees and this may be the first time they have sought such provision.

2.8. The present study

As identified above, there has been very little research detailing which cyber security controls have (or have not) been implemented by SMEs, with literature on cyber security controls suggesting that many SMEs lack basic cyber security controls, and often have no frameworks in place to guide implementation (Pawar & Palivela, 2022). There is an indication that smaller organizations may have fewer procedures in place to manage cyber security risks, although the detail of which procedures they may have in place is somewhat unknown. SMEs are also a heterogeneous population and vary in their general make up. For example, an SME may be private, public, government funded or charitable organization, will differ in size and will differ in maturity (e.g., they may be long established or could be a new startup). It is not currently clear whether the types of controls implemented by SMEs varies depending on the category of the SME. This level of detail can help in our understanding of which types of SMEs may be following best practices compared to others.

Research Question 1 (RQ1): *To what extent do the types of cyber security controls implemented vary across SME categories (i.e. size, type, maturity and sector)?*

Previous research has examined human factors related to SMEs' cyber security posture, such as awareness, knowledge, attitude and culture. There appears to be little consensus on whether there are variations within each of these factors amongst SMEs. One such reason could be that the heterogeneity amongst SMEs plays a role. However, minimal research to date has attempted to understand whether differences in these factors between SMEs varies on their specific make up (i.e. size, type, maturity, and sector).

Research Question 2 (RQ2): *To what extent do levels of awareness, knowledge, attitude and culture differ across SME categories (i.e. size, type, maturity and sector)?*

To overcome cyber security threats, it is important for SMEs to be aware of available support routes and how to engage with them. It is clear that SMEs do not tend to access those resources that are already available (e.g. cyber essentials), however little research has comprehensively investigated the types of resources SMEs may (or may not) be accessing and crucially the factors that influence this behavior. These areas of focus will be covered in the following two research questions.

Research Question 3 (RQ3): *To what extent do patterns of support use and support routes differ across SME categories (i.e. size, type, maturity and sector)?*

Research Question 4 (RQ4): *What are the factors that influence whether SMEs access resources to reduce their cyber security risk?*

Given the limited prior research systematically comparing SME cyber security practices across organizational categories, and consistent with recent work exploring cyber security in SME contexts (e.g., M. F. Arroyabe, C. F. A. Arranz,

I. Fernandez De Arroyabe, et al., 2024), the present study adopts an exploratory approach. The study examines patterns of variation across SME characteristics to identify areas where differences emerge and warrant further theoretical development.

3. Materials and methods

3.1. Participants

Participants were employees or owners of SMEs within various types of sectors as well as experts in cyber security. These participants were invited to take part because of their role in being able to comment upon their organization's experience of cyber security, as well as in seeking any related advice and support. The study specifically targeted SMEs across industries, as well as charities and sole traders (1–249 employees). In the UK, an SME is generally defined as an organization with fewer than 250 employees and an annual turnover not exceeding €50 million (approx. £44 m) and/or an annual balance sheet total not exceeding €43 million (approx. £38 m). The sample size for the qualitative data collection was based on population integrity in recruiting to lead into more targeted discussions during the interviews. In previous qualitative research studies where approximately 10–15 participants were interviewed, five to six interviews produced a significant proportion of the data, with most of the concepts identified within the first 10 interviews (Guest et al., 2006; Zhou et al., 2023).

A total of 374 participants completed the online survey and a subset of survey respondents ($N = 12$) were interviewed. The survey was conducted between November 2023 and April 2024 while the interviews were conducted during February–April 2024.

The 12 SMEs interviewed represented a range of sectors and varied in size. They included two sole traders in education and security (Participants 1 and 12). Micro businesses were represented by SMEs in information technology (5 employees), mental health (9 employees) and consultancy (9 employees) (Participants 2–4). Small SMEs included organizations in telecoms (10 employees), software development (13 employees) and technology (10 employees) (Participants 6, 9 and 11). The sample also included medium to larger SMEs, such as those in corporate travel management (50 employees), data protection (51 employees), IT services (100 employees) and logistics (160 employees) (Participants 5, 7, 8 and 10). To contextualize the qualitative sample, the size distribution of interview participants was compared with UK business population statistics. Nationally, the UK private sector is dominated by micro organizations, with around three quarters having no employees (aside from owners) and fewer than 1% employing 50–249 staff (Department for Business and Trade, 2025). The interview sample therefore includes a higher proportion of organizations in the 50–249 employee category than is reflected nationally.

Sectorally, relative to UK VAT/PAYE registered business distributions (Office for National Statistics, 2024), the interview sample includes a higher proportion of information technology – related organizations, while also representing professional services, education, health and social care, transport and engineering. Overall, the sample captures a range of SME contexts, although some sectors are more represented than in national distributions.

The participant distributions for the survey and interviews are in Tables 1 and 2. Table 3 presents the organizational characteristics and respondent roles of the 12 SMEs included in the qualitative interviews.

Table 1. Survey participants per organisation size.

SME Size	Number of participants
100–249 employees	60 (16%)
50–99 employees	56 (15%)
10–49 employees	122 (33%)
Under 10 employees	77 (21%)
Sole trader	59 (16%)
Total	374

Table 2. Interview participants per organisation size.

SME Size	Number of participants
100–249 employees	2 (17%)
50–99 employees	2 (17%)
10–49 employees	4 (33%)
Under 10 employees	2 (17%)
Sole trader	2 (17%)
Total	12

Table 3. Organisational characteristics and roles of interviewed SMEs.

Participant	Sector	Employees	Role in SME
P1	Education & Training	Sole trader	Founder
P2	Information Technology Services	5	Founder
P3	Health & Social Care	9	Operations Manager
P4	Professional Services	10	Founder
P5	Business Services	50	Chief Information Officer
P6	Information Technology Services	10	Founder
P7	Information Technology Services	100	IT Strategy Lead
P8	Transport & Logistics	160	IT Manager
P9	Information Technology Services	13	Co-Owner
P10	Professional Services	51	Founder
P11	Technology Services	10	Operations Lead
P12	Engineering & Technical Services	Sole trader	Sole Trader

3.2. Measures

A survey and a series of interviews were used as the main data collection methods. These aimed to: a) understand the support needs of SMEs; b) establish their current understanding and confidence around cyber security, and their awareness and perceptions of available support.

The survey captured core organizational constructs including knowledge, awareness, culture and capability as multifaceted domains represented by multiple individual indicators. Each facet was measured using a single direct item reflecting a specific organizational attribute, e.g., awareness of strong password practices, perceived knowledge level, leadership prioritization, or perceived capability to manage cyber security issues.

Each item was analyzed independently, as the research questions focused on variation across distinct aspects of organizational cyber security than on estimating underlying latent constructs. This approach allowed differential patterns to be identified across organizational categories. As indicators were analyzed individually instead of aggregated, internal consistency coefficients such as Cronbach's alpha were not applicable.

Content and face validity were supported through grounding in established cyber security and SME literature. The use of multiple indicators across each domain ensured coverage of distinct but related facets. Items were designed to reflect established dimensions of organizational cyber security and to capture concrete, interpretable organizational attributes relevant to SME practice.

3.3. Online survey

The online survey comprised 52 items organized into six thematic sections and delivered via Jisc Online Surveys. SMEs were recruited using a broad, non-industry-targeted approach. Participants were invited via the Prolific research platform, social media, project partner organizations, and snowball sampling. To be eligible, respondents needed to be an owner or decision-maker within a UK SME and able to comment on their organization's cyber security practices and/or experiences of seeking related advice and support. Completion of the survey took around 30 minutes, with participants having the opportunity to opt in to an interview at the end. The full questionnaire is provided in Appendix A. All items were developed after reviewing academic and practitioner sources and were reviewed by the project's advisory board, which included representatives from government and industry, to ensure clarity, contextual relevance and alignment with UK SME guidance.

Items relating to organizational demographics and characteristics (such as size, sector and respondent role) were aligned with the UK Cyber Security Breaches Survey (DSIT, 2024) to ensure compatibility with national SME classifications. Organizational maturity was measured as the self-described developmental stage of the business (e.g., early-stage start-up to industry leader), aligned to lifecycle and growth-stage distinctions discussed in the SME literature (OECD, 2023). Questions about cyber awareness and skills were based on research on employee knowledge, awareness, and training in cyber security (e.g., Alshaikh et al., 2021; Bada et al., 2015; Gundu, 2019; Li et al., 2022;

McCormac et al., 2017). Items addressing organizational attitude and culture were derived from prior research on cyber security culture and management commitment (e.g., Da Veiga, 2016; Georgiadou et al., 2022; Gerst et al., 2024; Uchendu et al., 2021) and from practical recommendations in the NCSC Small Business Guide (NCSC, 2020).

The questions about how well technical and procedural controls were put in place were based on the control families in the UK National Cyber Security Center's Cyber Essentials standard and the 10 Steps to Cyber Security framework (NCSC, 2020). These items (e.g. firewalls, secure configuration, user-access control, malware protection, and patch management) were supplemented with multi-factor authentication, backups, and mobile-device management, which are more recent recommendations for SMEs (e.g., Renaud & Ophoff, 2021; Renaud & Weir, 2016). The Cyber Security Breaches Survey taxonomy (DSIT, 2024) was the main source of information about online threats. Lists from ENISA (2021) and Verizon (2023) were also incorporated to make sure all the incidents that are most likely to impact SMEs were included.

Questions that asked about perceived support needs and experiences of seeking advice were based on research that looked at SME capability, confidence, and barriers to investing in cyber security (e.g., Alahmari & Duncan, 2021; Hoppe et al., 2021; Renaud & Ophoff, 2021). Finally, items concerning awareness and experience of different support routes were aligned with practitioner guidance and national programmes. such as those provided by the NCSC, IASME Cyber Assurance, Police Cyber Protect Officers, Regional Cyber Resilience Centres and the Information Commissioner's Office. These items captured not only awareness and usage but also satisfaction with the information and guidance received. Where items were adapted, wording was localized to the UK SME context while preserving the underlying construct intent. Practitioner-sourced items, such as those drawn from Cyber Essentials or NCSC materials, were retained verbatim where appropriate to maintain face validity.

3.4. Interviews

Online semi-structured interviews were also conducted to measure RQ4 (What are the factors that influence whether SMEs access resources to reduce their cyber security risk?), consisting of open-ended questions to encourage in-depth discussions (see Appendix B). The interviews comprised 17 items designed to explore SMEs' support needs, assess their knowledge and confidence in cyber security, and examine their awareness and perceptions of available support. Questions such as "What kind of support/guidance/advice has worked well in your experience? What hasn't worked well?" were asked. Interviews lasted between 28 and 50 minutes ($M = 40.16$). The licensed platform of Microsoft Teams was used. During the interviews no personal information of interviewees such as name, affiliation was shared, nor any attribution is made to any statements. Participants were provided with an information sheet before the interview and asked to provide their consent before participating. All questions asked focused on the experiences, knowledge and expertise of interviewees, while no personal questions were asked.

3.5. Data analysis

Data was analyzed using a mixed-method approach, utilizing quantitative and qualitative methods. For the survey analysis, a baseline descriptive analysis was undertaken to compare the findings from a sample of questions in the current survey with findings from comparative surveys (e.g. Cyber security breaches survey). This baseline analysis helps to understand whether survey respondents' answers are comparable when analyzing the results of the various Research Questions. The baseline analysis focused on 1) the priority SMEs give to cyber security (e.g. the priority cyber security is given by top management/owner), 2) their approach to cyber security (e.g. deployment of controls) and 3) their awareness (e.g. whether SMEs are providing regular cyber security training and awareness programmes to employees). One-way analysis of variance (ANOVAs), a statistical procedure used to test whether the means of three or more independent groups differ significantly (Field, 2017), were conducted to analyze the differences between SME size, type, maturity and sector with participant responses. Effect sizes were also presented for all ANOVA tests using partial eta squared (ηp^2) in addition to *p*-values. According to Cohen (1988), values of .01, .06, and .14 for ηp^2 correspond to small, medium, and large effects, respectively. Effect sizes and confidence intervals are presented alongside the ANOVA results. In addition to separate one-way ANOVAs, multivariable general linear models were estimated for each outcome variable to reduce reliance on isolated group comparisons. Organizational size, maturity, and sector were entered simultaneously as predictors. Effects were evaluated using Type II sums-of-squares F-tests, allowing each predictor to be assessed. Given the number of outcomes examined within each research question, *p*-values from ANOVA tests were adjusted using the Benjamini – Hochberg false discovery rate (FDR) procedure (q = .05) within each outcome (i.e. RQ1, RQ2, and RQ3 separately). Both raw and FDR-adjusted *p*-values are reported. Partial eta squared (ηp^2) and corresponding 95% confidence intervals are presented to support interpretation of practical significance. As the survey items were measured using 4- or 5-point Likert-type response scales (e.g., strongly disagree to strongly agree; not at all to a great extent) the responses were treated as approximately interval when scale categories are ordered, conceptually equidistant, and distributions do not exhibit extreme skew or floor/ceiling effects. Simulation and empirical research demonstrates that parametric tests such as ANOVA are robust to moderate violations of interval assumptions, particularly with larger sample sizes and approximately balanced group sizes (Field, 2017; Norman, 2010). In the present study, response distributions were inspected and did not demonstrate extreme floor or ceiling effects. Given the sample size ($N = 374$) and the robustness of ANOVA to non-normality under these conditions, Likert-type outcomes were analyzed using parametric procedures. To ensure findings were not dependent on distributional assumptions, sensitivity analyses were conducted using non-parametric Kruskal–Wallis tests for representative outcomes across RQ1–RQ3. The pattern of statistically significant and non-significant findings remained substantively unchanged. This indicates that conclusions were robust to ordinal-based analysis.

Size was defined using standard UK SME categories: sole trader, under 10 employees, 10–49 employees, 50–99 employees and 100–249 employees. Type referred to the organizational form (private business, public sector body, charity/nonprofit and government-funded organization). Maturity captured the stage of organizational development and was measured using five categories: early-stage start-up, growth-stage start-up, established organization, mature organization and industry leader (i.e. organizations that considered themselves among the most effective in their industry). Sector was measured using 18 industry categories (e.g., Construction, Education, Healthcare, Information Technology, and Retail). Post-hoc Tukey analysis was conducted to understand where the differences between the variables were. Chi-square analysis, a statistical procedure used to examine whether the frequency of cases in different categories differs from what would be expected by chance (Field, 2017), was conducted to understand whether there were significant differences between each of the variables of size, type, maturity and sector. For the interview analysis, to systematically analyze the narrative and identify patterns of themes, thematic analysis (Braun & Clarke, 2006) was utilized.

The qualitative strand formed an integral part of the study's convergent mixed-methods design. Its purpose was to provide interpretive and contextual depth to the quantitative findings rather than to develop an independent theoretical model. The interviews aimed to understand the reasons and processes behind the quantitative patterns found among SMEs. The two sets of data could therefore be compared and analyzed together to give a rounded picture of how SMEs behave in relation to cyber security. For the interview analysis, thematic analysis was utilized to systematically identify patterns within the narrative data (Braun & Clarke, 2006, 2021). The coding strategy was primarily inductive, allowing codes and themes to emerge from participants' accounts. However, the analysis was also informed by the focus of RQ4 and the broader mixed-methods design, meaning that coding remained attentive to the factors and processes that influence whether SMEs access cyber security support.

The analysis followed the six-step approach (Braun & Clarke, 2021): familiarization with the data, generation of initial codes, development of candidate themes, review and refinement of themes, definition and naming of themes, and writing up of the findings. Coding initially focused on explicit content in the data (e.g. not knowing where to seek support, perceptions of cost, skepticism toward providers), before codes were grouped into broader themes that captured recurring patterns across interviews. Initial open coding generated a broad set of 56 codes across the dataset, which were iteratively refined and consolidated into 33 codes. The final thematic structure comprised 33 codes, which were consolidated into 12 lower-order themes across seven higher-order themes (Table 10).

Two researchers independently reviewed and coded the interview transcripts to enhance the robustness of the analysis. The consensus coding approach was followed. Two researchers independently coded transcripts and met to discuss discrepancies until consensus was reached. Rather than seeking statistical inter-rater reliability, we adopted a reflexive thematic approach in which coding is viewed as an interpretative process. Regular discussions were held to refine themes and enhance analytic rigor. NVivo 14 was used to support data organization, coding, and theme development.

3.6. *Ethical considerations*

This study was reviewed and approved by Queen Mary University of London ethics committee with the approval number: PSY2023-33, dated 30–10-2023. Participants were informed of the aims and objectives of this study and informed consent was acquired before their participation. Participants were able to withdraw their data during or after the study. Participants were also debriefed at the end of their participation and were assured of their right to withdraw at any point up until the submission of their responses or until the data analysis stage commenced for the interview.

An overview of the study design and analysis process is presented in Figure 1.

4. Results

In measuring the baseline findings compared to the UK Cyber Breaches Survey 2025, 25% of the study participants said that cyber security is not a priority amongst management, which is aligned with the 2025 Cyber Breaches Survey which also reported that 28% of overall organizations do not see it as a high priority. The most frequently used controls by SMEs were a strong passwords policy ($M = 3.34$), backup ($M = 3.26$) and user access control ($M = 3.17$) which were all amongst the top six most frequently cited controls in the 2025 Cyber Breaches Survey. 41% of SMEs provided regular cyber security training and awareness programmes to employees, which also aligns to the 2025 Cyber Breaches Survey (34% for small business; 54% for medium businesses). The chi-square analysis indicated there was no significant differences ($p > .05$) between each of the measured variables of Size, Type, Maturity and Sector.

4.1. *RQ1. To what extent do the types of cyber security controls implemented vary across SME categories (i.e. size, type, maturity, and sector)?*

To examine RQ1, which explored the extent to which the types of cyber security controls implemented vary across SME categories (i.e. size, type, maturity and sector), one-way ANOVAs were conducted on the presence of cyber security controls implemented. When analyzing organization size, there was a significant effect for mobile device management ($F(4, 332) = 2.95$, $p < .05$, $\eta p^2 = 0.034$ [0.001, 0.071]), strong passwords policy ($F(4, 358) = 2.45$, $p < .05$, $\eta p^2 = 0.027$ [0.000, 0.058]), an agreed process for staff to follow with fraudulent e-mails or websites ($F(4, 356) = 2.45$, $p < .05$, $\eta p^2 = 0.035$ [0.002, 0.071]) and rules for storing and moving personal data securely ($F(4, 351) = 3.15$, p

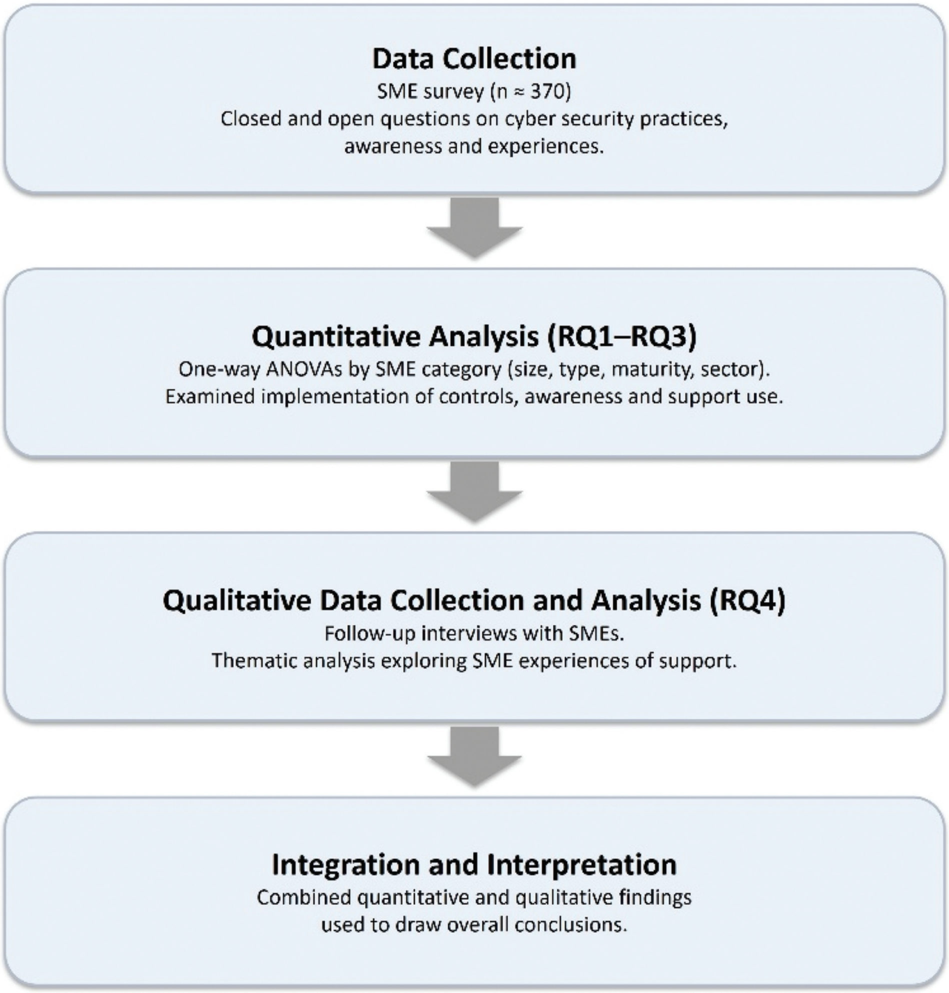
Data Collection
SME survey (n ≈ 370)
Closed and open questions on cyber security practices, awareness and experiences.
Quantitative Analysis (RQ1–RQ3)
One-way ANOVAs by SME category (size, type, maturity, sector).
Examined implementation of controls, awareness and support use.
Qualitative Data Collection and Analysis (RQ4)
Follow-up interviews with SMEs.
Thematic analysis exploring SME experiences of support.
Integration and Interpretation
Combined quantitative and qualitative findings used to draw overall conclusions.

Figure 1. Overview of the study design and analysis process. The figure shows the sequence of data collection, quantitative and qualitative analyses, and the integration of findings across the four research questions (RQ1–RQ4). Data were collected through a survey of SMEs containing closed and open questions on cyber security practices, awareness and experiences, followed by interviews analysed thematically to explore SME support experiences.

$< .05$, $\eta p^2 = 0.035$ [0.001, 0.071]). Post hoc Tukey test results reveal that organizations with 100–249 employees had lower use of mobile device management ($M = 2.20$, SD = 1.07) than all other organization sizes and a significantly lower use of mobile device management than organizations with 50–99 employees ($M = 2.80$, SD = 1.07) and 10–49 employees ($M = 2.65$, SD = 0.88). Organizations with 100–249 employees had a significantly lower score on agreed process for staff to follow with fraudulent e-mails or websites than all other organization sizes ($M = 2.29$, SD = 1.20) and was significantly lower than organizations with 10–49 employees ($M = 2.89$, SD = 1.20). Organizations with 100–249 employees also had a significantly lower score on rules for storing and moving personal data securely ($M = 2.38$, SD = 1.17) than organizations with 10–49 employees ($M = 2.94$, SD = 1.02). There was also a significant effect for whether the organization provides regular training and awareness programmes to employees ($F(4, 368) = 2.64$, $p < .05$, $\eta p^2 = 0.028$ [0.000, 0.060]), whether organizations have a formal policy or policies covering cyber security risks ($F(4, 329) = 2.44$, $p < .05$, $\eta p^2 = 0.029$ [0.000, 0.063]) and had separate Wi-Fi for staff and visitors ($F(4, 339) = 5.51$, $p < .05$, $\eta p^2 = 0.061$ [0.015, 0.108]). Sole Traders had a lower amount of regular training and awareness programmes than all other organization sizes and post hoc Tukey test results reveal there was

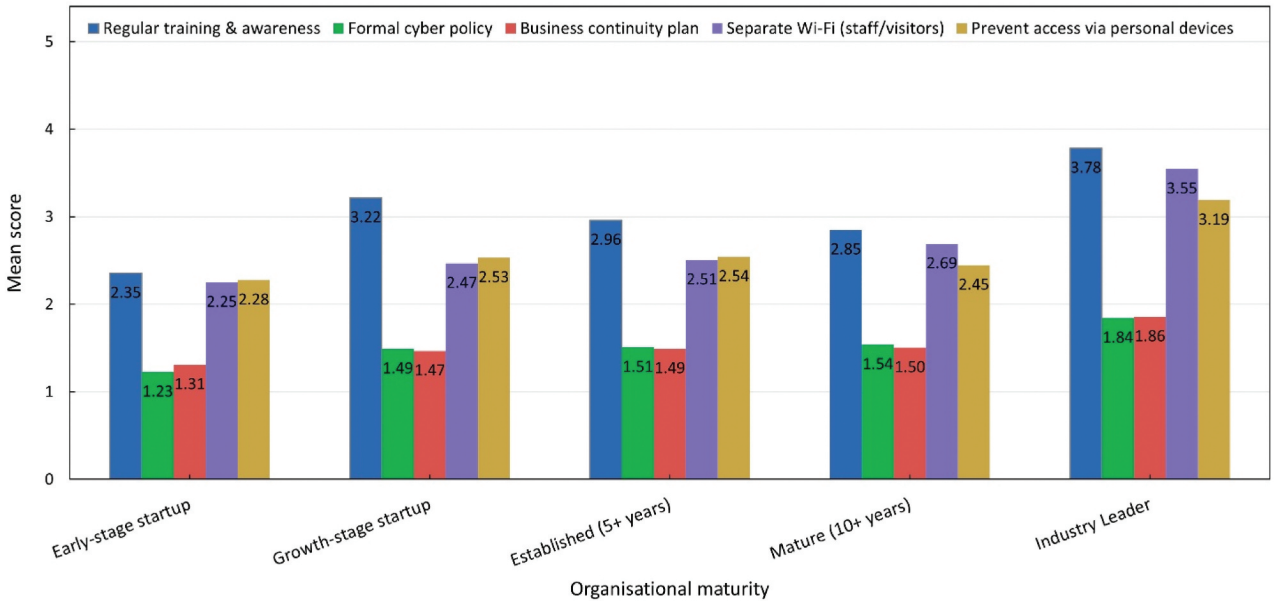

Figure 2. Implementation of five cyber-security controls by organisational maturity (means). Scores increase notably between early-stage to industry-leading SMEs for regular training and awareness, formal policy or policies covering cyber security risks, business-continuity planning, Wi-Fi for staff and visitors, and controls to prevent access via personally owned devices.

a significant difference between Sole Traders (M = 2.86, SD = 1.38) and organizations with 50–99 employees (M = 3.93, SD = 1.141). Organizations with 100–249 employees had a higher mean score for separate Wi-Fi for staff and visitors than all other organization sizes with post hoc test results revealing there was a significant difference between this organization size (M = 3.80, SD = 0.42) and sole traders (M = 2.52, SD = 1.31).

There were no significant effects for organization type. When analyzing the maturity of an organization, there was a significant effect for providing regular cyber security training and awareness programmes to employees (F(4, 369) = 4.54, $p < .05$, $\eta p^2 = 0.047$ [0.008, 0.087]), a formal policy or policies covering cyber security risks (F(4, 330) = 4.97, $p < .01$, $\eta p^2 = 0.057$ [0.012, 0.103]), a business continuity plan that covers cyber security (F(4, 297) = 2.94, $p < .05$, $\eta p^2 = 0.038$ [0.001, 0.079]), separate Wi-Fi for staff and visitors (F(4, 340) = 3.79, $p < .05$, $\eta p^2 = 0.043$ [0.005, 0.083]) and preventing access via personally owned devices (F(4, 348) = 2.43, $p < .05$, $\eta p^2 = 0.027$ [0.000, 0.060]). Post hoc Tukey test results reveal that Industry Leader organizations have a higher level of regular cyber security training and awareness programmes to employees (M = 3.78, SD = 1.48) and a significantly higher level than early stage start-ups (M = 2.35, SD = 1.25). Industry leader organizations also have a higher mean score on having a formal policy or policies covering cyber security risks (M = 1.84, SD = 0.38) compared to other organizations and a significantly higher level than early stage startups (M = 1.23, SD = 0.43). Mature organizations also had a significantly higher mean score on having a formal policy or policies covering cyber security risks (M = 1.54, SD = 0.50). Industry leader organizations also had a significantly higher mean score when asked whether they had a business continuity plan that covers cyber security (M = 1.86, SD = 0.36) compared with early-stage startups (M = 1.31, SD = 0.47). When analyzing whether organizations have separate WiFi for staff and visitors, Industry Leader organizations reported a significantly higher difference (M = 3.55, SD = 0.91) than Mature organizations (M = 2.69, SD = 1.30), Established organizations (M = 2.51, SD = 1.34), Growth-stage startups (M = 2.47, SD = 1.34) and Early-stage startups (M = 2.25, SD = 1.30). Industry Leader organizations (M = 3.55, SD = 0.91) also had a significantly higher score than Growth-stage startups ($M = 2.47$, SD = 1.34). Industry Leader organizations also had a significantly higher mean score on preventing access via personally owned devices ($M = 3.19$, SD = 0.93) than Early-stage startups ($M = 2.28$, SD = 1.28).

Figure 2 illustrates the relationship between organizational maturity and the implementation of cyber-security controls, showing a clear upward trend between early-stage startup and industry leader SMEs.

When analyzing the sector of an organization, the Information Technology industry was higher than all other sectors. There was a significant effect for Firewalls ($F(17, 327) = 2.66$, $p < .05$, $\eta p^2 = 0.102$ [0.018, 0.135]), Secure configuration ($F(17, 326) = 2.42$, $p < .05$, $\eta p^2 = 0.094$ [0.012, 0.124]), User access control ($F(17, 333) = 2.49$, $p < .05$, $\eta p^2 = 0.095$ [0.014, 0.125]), Malware protection ($F(17, 335) = 2.17$, $p < .05$, $\eta p^2 = 0.083$ [0.006, 0.110]), Patch management ($F(17, 301) = 2.88$, $p < .01$, $\eta p^2 = 0.118$ [0.026, 0.155]), Anti-phishing ($F(17, 313) = 3.07$, $p < .01$, $\eta p^2 = 0.121$ [0.030, 0.158]), User education ($F(17, 339) = 3.55$, $p < .01$, $\eta p^2 = 0.128$ [0.040, 0.166]), Backup ($F(17, 337) = 2.66$, $p < .01$, $\eta p^2 = 0.100$ [0.018, 0.131]), Data encryption ($F(17, 324) = 3.72$, $p < .01$, $\eta p^2 = 0.138$ [0.046, 0.180]), Mobile device management ($F(17, 318) = 2.67$, $p < .01$, $\eta p^2 = 0.105$ [0.019, 0.138]), Cloud network security ($F(17, 309) = 4.72$, $p < .01$, $\eta p^2 = 0.176$ [0.076, 0.224]), Separate Wi-Fi for staff and visitors ($F(17, 325) = 2.22$, $p < .05$, $\eta p^2 = 0.087$ [0.007, 0.115]), An agreed process for staff to follow with fraudulent e-mails or websites ($F(17, 342) = 4.37$, $p < .01$, $\eta p^2 = 0.152$ [0.061, 0.195]), Rules for storing and moving personal data securely ($F(17, 337) = 4.27$, $p < .01$, $\eta p^2 = 0.151$ [0.059, 0.194]), Monitoring of user activity ($F(17, 329) = 2.65$, $p < .05$, $\eta p^2 = 0.101$ [0.018, 0.133]), and A policy to apply software security updates within 14 days ($F(17, 303) = 3.06$, $p < .01$, $\eta p^2 = 0.124$ [0.031, 0.162]). The full one-way ANOVA results for RQ1 are presented in Table 4.

Table 4. RQ1 one-way ANOVA results.

Types of controls implemented by SMEs				
Organisation Size				
Control	**F**	**df**	**p**	**ηp^2 [95% CI]**
Mobile device management	2.95	4, 332	<0.05	0.034 [0.001, 0.071]
Strong passwords policy	2.45	4, 358	<0.05	0.027 [0.000, 0.058]
An agreed process for staff to follow with fraudulent emails or websites	2.45	4, 356	<0.05	0.035 [0.002, 0.071]
Rules for storing and moving personal data securely	3.15	4, 351	<0.05	0.035 [0.001, 0.071]
Provides regular training and awareness programmes to employees	2.64	4, 368	<0.05	0.028 [0.000, 0.060]
Formal policy or policies covering cyber security risks	2.44	4, 329	<0.05	0.029 [0.000, 0.063]
Separate Wi-Fi for staff and visitors	5.51	4, 339	<0.05	0.061 [0.015, 0.108]
Maturity of organisation				
Control	**F**	**df**	**p**	**ηp^2 [95% CI]**
Provides regular training and awareness programmes to employees	4.54	4, 369	<0.05	0.047 [0.008, 0.087]
Formal policy or policies covering cyber security risks	4.97	4, 330	<0.01	0.057 [0.012, 0.103]
Business continuity plan that covers cyber security	2.94	4, 297	<0.05	0.038 [0.001, 0.079]
Separate Wi-Fi for staff and visitors	3.79	4, 340	<0.05	0.043 [0.005, 0.083]
Preventing access via personally owned devices	2.43	4, 348	<0.05	0.027 [0.000, 0.060]
Sector of organisation				
Control	**F**	**df**	**p**	**ηp^2 [95% CI]**
Firewalls	2.66	17, 327	<0.05	0.102 [0.018, 0.135]
Secure configuration	2.42	17, 326	<0.05	0.094 [0.012, 0.124]
User access control	2.49	17, 333	<0.05	0.095 [0.014, 0.125]
Malware protection	2.17	17, 335	<0.05	0.083 [0.006, 0.110]
Patch management	2.88	17, 301	<0.01	0.118 [0.026, 0.155]
Anti-phishing	3.07	17, 313	<0.01	0.121 [0.030, 0.158]
User education	3.55	17, 339	<0.01	0.128 [0.040, 0.166]
Backup	2.66	17, 337	<0.01	0.100 [0.018, 0.131]
Data encryption	3.72	17, 324	<0.01	0.138 [0.046, 0.180]
Mobile device management	2.67	17, 318	<0.01	0.105 [0.019, 0.138]
Cloud network security	4.72	17, 309	<0.01	0.176 [0.076, 0.224]
Separate Wi-Fi for staff and visitors	2.22	17, 325	<0.05	0.087 [0.007, 0.115]
An agreed process for staff to follow with fraudulent emails or websites	4.37	17, 342	<0.01	0.152 [0.061, 0.195]
Rules for storing and moving personal data securely	4.27	17, 337	<0.01	0.151 [0.059, 0.194]
Monitoring of user activity	2.65	17, 329	<0.05	0.101 [0.018, 0.133]
A policy to apply software security updates within 14 days	3.06	17, 303	<0.01	0.124 [0.031, 0.162]

In addition to the separate one-way ANOVAs, multivariable general linear models were estimated for each control implementation outcome to examine the independent contribution of organizational size, maturity and sector when entered simultaneously. Effects were evaluated using Type II sums-of-squares F-tests, allowing each predictor to be assessed while adjusting for the others. Given the number of outcomes examined within RQ1, *p*-values were adjusted using the Benjamini – Hochberg false discovery rate procedure ($q = .05$). Table 5 reports full model statistics, including F-tests, FDR-adjusted *p*-values and effect sizes (ηp^2).

When organizational size, maturity and sector were analyzed simultaneously, sector emerged as the most consistent independent predictor of control implementation. After FDR correction, significant sector effects were observed across a broad range of governance, technical and procedural controls. These included regular training and awareness programmes ($\eta p^2 = .157$), formal cyber security policies ($\eta p^2 = .148$), business continuity planning ($\eta p^2 = .112$), firewalls ($\eta p^2 = .124$), secure configuration ($\eta p^2 = .117$), user access control ($\eta p^2 = .106$), malware protection ($\eta p^2 = .087$), patch management ($\eta p^2 = .134$), anti-phishing controls ($\eta p^2 = .118$), user education ($\eta p^2 = .124$), backup ($\eta p^2 = .104$), data encryption ($\eta p^2 = .124$), mobile device management ($\eta p^2 = .101$), cloud network security ($\eta p^2 = .169$), agreed processes for responding to fraudulent e-mails or websites ($\eta p^2 = .147$), rules for secure data handling ($\eta p^2 = .147$), monitoring of user activity ($\eta p^2 = .097$), and policies to apply software security updates within 14 days ($\eta p^2 = .137$). Sector effects were generally small to moderate in magnitude, with comparatively larger effects observed for cloud network security ($\eta p^2 = .169$), formal policy ($\eta p^2 = .148$), agreed processes ($\eta p^2 = .147$), secure data handling rules ($\eta p^2 = .147$), and patch management ($\eta p^2 = .134$). This pattern indicates that sectoral context plays a substantive role in shaping both technical infrastructure and governance-oriented control adoption, even when organizational size and maturity are accounted for.

Organizational size also demonstrated broad independent associations following FDR correction. Significant size effects were observed for governance-oriented controls, including regular training and awareness programmes ($\eta p^2 = .076$), formal policy ($\eta p^2 = .158$), business continuity planning ($\eta p^2 = .159$), and separate Wi-Fi provision for staff and visitors ($\eta p^2 = .118$). Size additionally retained significant associations with several technical and operational controls, including firewalls ($\eta p^2 = .035$), secure configuration ($\eta p^2 = .052$), anti-phishing measures ($\eta p^2 = .048$), user education ($\eta p^2 = .043$), strong passwords policies ($\eta p^2 = .034$), data encryption ($\eta p^2 = .061$), mobile device management ($\eta p^2 = .069$), cloud network security ($\eta p^2 = .061$), monitoring of user activity ($\eta p^2 = .054$), agreed processes for fraudulent e-mails or websites ($\eta p^2 = .036$), rules for secure data handling ($\eta p^2 = .057$), policies to apply software updates within 14 days ($\eta p^2 = .052$), and preventing access via personally owned devices ($\eta p^2 = .062$). Although effect sizes were generally modest, the strongest size effects were observed for formal policy and business continuity planning (both $\eta p^2 \approx .16$), suggesting that organizational scale is particularly relevant for the adoption of structured governance mechanisms and resilience planning.

In contrast, organizational maturity demonstrated substantially attenuated effects once size and sector were included in the model. Following FDR correction, maturity retained a statistically significant independent association only with mobile device management ($\eta p^2 = .038$). All other maturity effects were reduced to non-significance. This pattern suggests that maturity-related differences observed in the one-way ANOVAs may partly reflect underlying variation associated with sectoral composition and organizational scale, rather than maturity alone exerting an independent influence on control implementation.

Overall, the multivariable results indicate that variation in control implementation is structured predominantly by sector, with organizational size contributing to differences in governance formalization and selected technical safeguards, and organizational maturity playing a more limited and specific role once structural characteristics are taken into account.

Table 5. RQ1 multivariable results.

Multivariable predictors of cyber security controls					
Outcome	Predictor	F(df1, df2)	p	p(FDR)	ηp^2
Provides regular training and awareness programmes to employees	Size	7.13 (4, 348)	<.001	<.001	.076
	Maturity	2.63 (4, 348)	.034	.057	.029
	Sector	3.82 (17, 348)	<.001	<.001	.157
Formal policy or policies covering cyber security risks	Size	14.51 (4, 309)	<.001	<.001	.158
	Maturity	0.82 (4, 309)	.515	.646	.010
	Sector	3.16 (17, 309)	<.001	<.001	.148
Business continuity plan that covers cyber security	Size	13.15 (4, 278)	<.001	<.001	.159
	Maturity	0.55 (4, 278)	.699	.778	.008
	Sector	2.33 (17, 278)	.004	.009	.112
Firewalls	Size	2.95 (4, 321)	.020	.037	.035
	Maturity	0.63 (4, 321)	.644	.740	.008
	Sector	2.84 (17, 321)	<.001	.001	.124
Secure configuration	Size	4.38 (4, 320)	.002	.005	.052
	Maturity	0.63 (4, 320)	.641	.740	.008
	Sector	2.49 (17, 320)	.001	.003	.117
User access control	Size	0.85 (4, 327)	.496	.633	.010
	Maturity	0.71 (4, 327)	.589	.701	.009
	Sector	2.27 (17, 327)	.003	.008	.106
Malware protection	Size	0.78 (4, 329)	.536	.657	.009
	Maturity	0.43 (4, 329)	.787	.848	.005
	Sector	1.95 (17, 329)	.016	.031	.087
Patch management	Size	1.93 (4, 295)	.105	.162	.025
	Maturity	0.20 (4, 295)	.936	.936	.003
	Sector	2.86 (17, 295)	<.001	.001	.134
Anti-Phishing	Size	3.89 (4, 307)	.004	.010	.048
	Maturity	1.49 (4, 307)	.205	.295	.019
	Sector	2.58 (17, 307)	<.001	.003	.118
User education	Size	3.70 (4, 333)	.006	.013	.043
	Maturity	1.32 (4, 333)	.261	.368	.016
	Sector	2.76 (17, 333)	<.001	.001	.124
Backup	Size	2.68 (4, 331)	.032	.055	.031
	Maturity	1.16 (4, 331)	.329	.445	.014
	Sector	2.26 (17, 331)	.003	.008	.104
Data encryption	Size	5.17 (4, 318)	<.001	.002	.061
	Maturity	0.77 (4, 318)	.543	.657	.010
	Sector	2.65 (17, 318)	<.001	.002	.124
Mobile Device Management	Size	5.80 (4, 312)	<.001	<.001	.069
	Maturity	3.09 (4, 312)	.016	.031	.038
	Sector	2.06 (17, 312)	.008	.018	.101
Strong passwords policy	Size	2.95 (4, 338)	.020	.037	.034
	Maturity	0.89 (4, 338)	.470	.612	.010
	Sector	1.28 (17, 338)	.201	.294	.061
Cloud Network Security	Size	4.94 (4, 303)	<.001	.002	.061
	Maturity	1.86 (4, 303)	.118	.177	.024
	Sector	3.63 (17, 303)	<.001	<.001	.169
Separate Wi-Fi for staff and visitors	Size	10.69 (4, 319)	<.001	<.001	.118
	Maturity	0.52 (4, 319)	.725	.794	.006
	Sector	1.72 (17, 319)	.038	.062	.084
Preventing access via personally owned devices	Size	5.37 (4, 327)	<.001	.001	.062
	Maturity	1.29 (4, 327)	.272	.375	.016
	Sector	1.51 (17, 327)	.090	.141	.073
An agreed process for staff to follow with fraudulent emails or websites	Size	3.12 (4, 336)	.015	.031	.036
	Maturity	0.26 (4, 336)	.904	.936	.003
	Sector	3.40 (17, 336)	<.001	<.001	.147
Rules for storing and moving personal data securely	Size	4.96 (4, 331)	<.001	.002	.057
	Maturity	0.22 (4, 331)	.926	.936	.003
	Sector	3.36 (17, 331)	<.001	<.001	.147
Monitoring of user activity	Size	4.62 (4, 323)	.001	.004	.054
	Maturity	0.40 (4, 323)	.806	.856	.005
	Sector	2.32 (17, 323)	.004	.009	.097
A policy to apply software security updates within 14 days	Size	4.09 (4, 297)	.003	.008	.052
	Maturity	0.21 (4, 297)	.933	.936	.003
	Sector	2.96 (17, 297)	<.001	<.001	.137

4.2. RQ2. To what extent do levels of awareness, knowledge, attitude, and culture differ across SME categories (i.e. size, type, maturity, and sector)?

To examine RQ2, which aimed to explore the extent to which levels of awareness, knowledge, attitude and culture differ across SME categories (i.e. size, type, maturity and sector), one-way ANOVAs were conducted. There were no significant effects of SME size or type on the variable of interest. For maturity of the SME, there was a significant effect for concern about cyber security ($F(4, 364) = 4.38$, $p < .05$, $\eta p^2 = 0.046$ [0.007, 0.086]), interest in addressing cyber security ($F(4, 365) = 3.12$, $p < .05$, $\eta p^2 = 0.033$ [0.001, 0.068]), and capability to handle cyber security issues ($F(4, 357) = 2.45$, $p < .05$, $\eta p^2 = 0.027$ [0.000, 0.059]). Post hoc Tukey tests reveal that Industry Leader organizations had a significantly greater concern for cyber security ($M = 3.85$, $SD = 1.17$) than Early-stage start-ups ($M = 2.73$, $SD = 1.24$). Industry Leader organizations also had a significantly greater capability to handle cyber security issues ($M = 3.75$, $SD = 1.19$) than Early-stage start-ups ($M = 2.70$, SD 1.37).

Figure 3 shows the relationship between SME maturity and cyber-security concern, interest and capability. Mean scores for concern, interest, and capability increase between early-stage to industry-leading SMEs, indicating that more mature organizations show both heightened recognition of cyber risk and stronger capacity to respond effectively.

When analyzing organization sector, the Information Technology sector had a significant effect for providing regular cyber security training and awareness programmes to employees ($F(17, 354) = 4.86$, $p < .001$, $\eta p^2 = 0.161$ [0.071, 0.206]), the general level of knowledge on cyber security ($F(17, 354) = 4.82$, $p < .001$, $\eta p^2 = 0.160$ [0.070, 0.204]), employees trained on how to identify phishing e-mails and other social engineering attacks ($F(17, 350) = 2.19$, $p < .05$, $\eta p^2 = 0.081$ [0.006, 0.106]), employees know how to report cyber security incidents or suspicious activities ($F(17, 345) = 2.01$, $p < .05$, $\eta p^2 = 0.075$ [0.002, 0.099]), cyber security is seen as a priority by top management/owner ($F(17, 342) = 3.34$, $p < .001$, $\eta p^2 = 0.120$ [0.034, 0.157]), understanding cyber security ($F(17, 352) = 4.78$, $p < .001$, $\eta p^2 = 0.160$ [0.069, 0.204]), concern about it ($F(17, 349) = 4.34$, $p < .001$, $\eta p^2 = 0.148$ [0.059, 0.191]), interest in addressing it ($F(17, 350) = 3.76$, $p < .001$, $\eta p^2 = 0.131$ [0.044, 0.170]), budget priority ($F(17, 335) = 4.01$, $p < .001$, $\eta p^2 = 0.144$ [0.052, 0.185]),

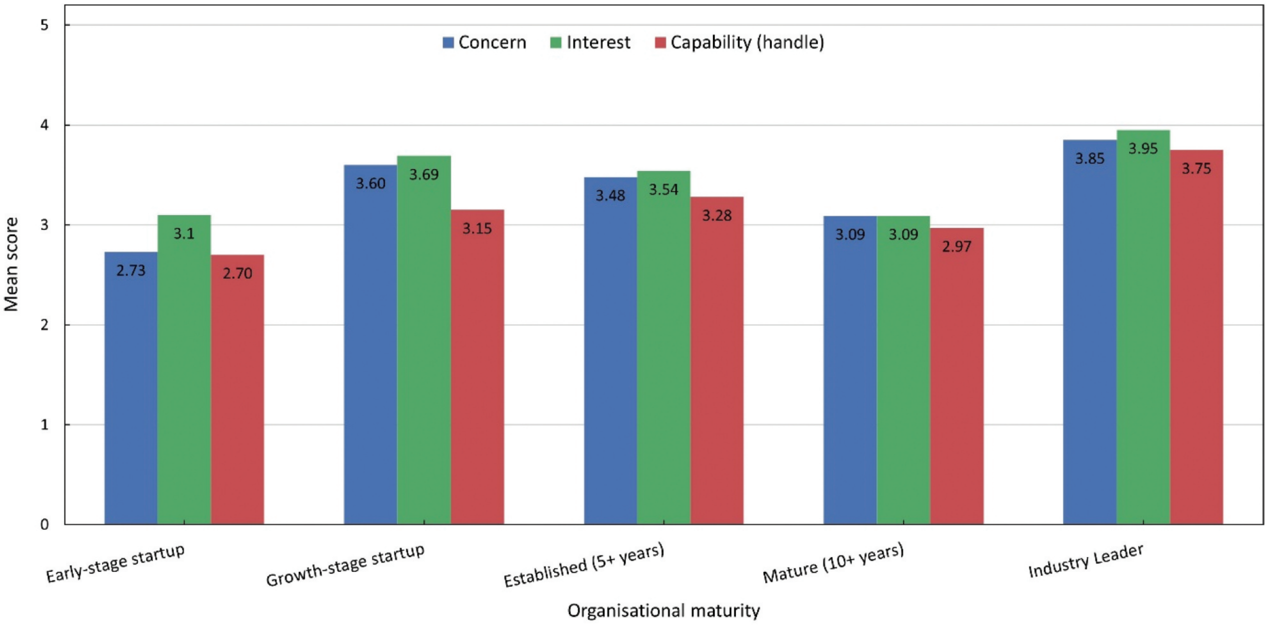

Figure 3. Mean concern, interest, and capability to handle cyber-security issues by SME maturity (means). Scores increase notably between early-stage startups and industry-leading SMEs.

capability to prevent cyber security issues ($F(17, 343) = 6.19$, $p < .001$, $\eta p^2 = 0.202$ [0.106, 0.252]), capability to identify cyber security issues ($F(17, 348) = 4.52$, $p < .001$, $\eta p^2 = 0.154$ [0.063, 0.197]) and capability to handle cyber security issues ($F(17, 342) = 4.35$, $p < .001$, $\eta p^2 = 0.151$ [0.060, 0.194]). The full one-way ANOVA results for RQ2 are presented in Table 6.

In addition to the separate one-way ANOVAs reported above, multivariable general linear models were estimated for each awareness, knowledge, attitude and culture outcome to examine the independent contribution of organizational size, maturity and sector when entered simultaneously. Effects were evaluated using Type II sums-of-squares F-tests, allowing each predictor to be assessed while adjusting for the others. Given the number of outcomes examined within RQ2, p-values were adjusted using the Benjamini – Hochberg false discovery rate (FDR) procedure (q = .05). Full model statistics, including F-tests, FDR-adjusted p-values and effect sizes (ηp^2), are reported in Table 7.

When organizational size, maturity and sector were analyzed simultaneously, sector emerged as the most consistent predictor across awareness, knowledge, attitudinal, and capability outcomes. After FDR correction, significant sector effects were observed for general level of knowledge on cyber security ($\eta p^2 = .165$), cyber security being seen as a priority by top management/owner ($\eta p^2 = .130$), understanding cyber security ($\eta p^2 = .170$), concern about cyber security ($\eta p^2 = .172$), interest in addressing cyber security ($\eta p^2 = .151$), budget priority ($\eta p^2 = .150$), capability to prevent cyber security issues ($\eta p^2 = .210$), capability to identify cyber security issues ($\eta p^2 = .170$), and capability to handle cyber security issues ($\eta p^2 = .166$). Sector effects were generally small-to-moderate in magnitude, with comparatively larger effects observed for capability to prevent cyber security issues ($\eta p^2 = .210$), concern about cyber security ($\eta p^2 = .172$), and understanding cyber security ($\eta p^2 = .170$).

Organizational size also retained independent associations following adjustment and FDR correction. Significant size effects were observed for general level of knowledge on cyber security ($\eta p^2 = .037$) and employees being trained on how to identify phishing e-mails and other social engineering attacks ($\eta p^2 = .042$). Size also remained independently associated with capability outcomes, including capability to prevent cyber security issues ($\eta p^2 = .036$), capability to identify cyber security issues ($\eta p^2 = .052$), and capability to handle cyber security issues ($\eta p^2 = .051$). Size effects were small in magnitude overall, with comparatively larger effects observed for capability to identify and handle cyber security issues.

Table 6. RQ2 one-way ANOVA results.

	The extent that an SMEs category varies in their levels of awareness, knowledge, attitude and culture			
	Maturity of organisation			
Awareness, knowledge, attitude and culture	**F**	**df**	**p**	**ηp^2 [95% CI]**
Concern about it	4.38	4, 364	<0.05	0.046 [0.007, 0.086]
Interest in addressing cyber security	3.12	4, 365	<0.05	0.033 [0.001, 0.068]
Capability to handle cyber security issues	2.45	4, 357	<0.05	0.027 [0.000, 0.059]
	Sector of organisation			
Awareness, knowledge, attitude and culture	**F**	**df**	**p**	**ηp^2 [95% CI]**
General level of knowledge on cyber security	4.82	17, 354	<0.001	0.160 [0.070, 0.204]
Employees trained on how to identify phishing emails and other social engineering attacks	2.19	17, 350	<0.05	0.081 [0.006, 0.106]
Employees know how to report cyber security incidents or suspicious activities	2.01	17, 345	<0.05	0.075 [0.002, 0.099]
Cyber security is seen as a priority by top management/owner	3.34	17, 342	<0.001	0.120 [0.034, 0.157]
Understanding cyber security	4.78	17, 352	<0.001	0.160 [0.069, 0.204]
Concern about it	4.34	17, 349	<0.001	0.148 [0.059, 0.191]
Interest in addressing it	3.76	17, 350	<0.001	0.131 [0.044, 0.170]
Budget priority	4.01	17, 335	<0.001	0.144 [0.052, 0.185]
Capability to prevent cyber security issues	6.19	17, 343	<0.001	0.202 [0.106, 0.252]
Capability to identify cyber security issues	4.52	17, 348	<0.001	0.154 [0.063, 0.197]
Capability to handle cyber security issues	4.35	17, 342	<0.001	0.151 [0.060, 0.194]

Table 7. RQ2 multivariable results.

Multivariable predictors of awareness, knowledge, attitude and culture outcomes					
Outcome	Predictor	F(df1, df2)	p	p(FDR)	ηp^2
General level of knowledge on cyber security	Size	3.38 (4, 348)	.010	.026	.037
	Maturity	2.00 (4, 348)	.094	.137	.022
	Sector	4.04 (17, 348)	<.001	<.001	.165
Employees trained on how to identify phishing emails and other social engineering attacks	Size	3.73 (4, 344)	.005	.015	.042
	Maturity	1.21 (4, 344)	.306	.389	.014
	Sector	1.77 (17, 344)	.031	.060	.080
Employees know how to report cyber security incidents or suspicious activities	Size	2.10 (4, 339)	.080	.120	.024
	Maturity	0.28 (4, 339)	.889	.889	.003
	Sector	1.78 (17, 339)	.029	.060	.082
Cyber security is seen as a priority by top management/owner	Size	2.40 (4, 336)	.050	.083	.028
	Maturity	0.82 (4, 336)	.513	.552	.010
	Sector	2.96 (17, 336)	<.001	<.001	.130
Understanding cyber security	Size	2.64 (4, 346)	.034	.060	.030
	Maturity	1.16 (4, 346)	.327	.398	.013
	Sector	4.17 (17, 346)	<.001	<.001	.170
Concern about it	Size	1.15 (4, 343)	.332	.398	.013
	Maturity	4.03 (4, 343)	.003	.010	.045
	Sector	4.20 (17, 343)	<.001	<.001	.172
Interest in addressing it	Size	2.25 (4, 344)	.064	.103	.025
	Maturity	2.74 (4, 344)	.029	.060	.031
	Sector	3.59 (17, 344)	<.001	<.001	.151
Budget priority	Size	2.20 (4, 329)	.068	.106	.026
	Maturity	1.63 (4, 329)	.166	.233	.019
	Sector	3.43 (17, 329)	<.001	<.001	.150
Capability to prevent cyber security issues	Size	3.16 (4, 337)	.014	.036	.036
	Maturity	2.63 (4, 337)	.034	.060	.030
	Sector	5.28 (17, 337)	<.001	<.001	.210
Capability to identify cyber security issues	Size	4.73 (4, 342)	.001	.004	.052
	Maturity	1.22 (4, 342)	.302	.389	.014
	Sector	4.13 (17, 342)	<.001	<.001	.170
Capability to handle cyber security issues	Size	4.50 (4, 336)	.001	.005	.051
	Maturity	1.53 (4, 336)	.192	.260	.018
	Sector	3.92 (17, 336)	<.001	<.001	.166

In contrast, organizational maturity demonstrated more limited independent effects once size and sector were included in the model. Following FDR correction, maturity retained a statistically significant association only with concern about cyber security ($\eta p^2 = .045$). Maturity effects observed in the one-way ANOVAs for other awareness, knowledge and capability outcomes did not remain significant after adjusting for sector and organizational size.

Overall, the multivariable results for RQ2 indicate that variation in awareness, knowledge, attitude and capability is structured predominantly by sector, with organizational size contributing modestly to differences in general knowledge, phishing training and perceived capability, and organizational maturity playing a more specific role in shaping levels of concern.

4.3. RQ3. To what extent do patterns of support use and support routes differ across SME categories (i.e. size, type, maturity, and sector)?

To examine RQ3, which explored the extent to which patterns of support use and support routes differ across SME categories, one-way ANOVAs were conducted on the presence of support routes. When analyzing organization size, there was a significant effect for ISO 27001 ($F(4, 362) = 3.461$, $p < .01$, $\eta p^2 = 0.037$ [0.003, 0.074]), PCI Data Security Standard (DSS) ($F(4, 364) = 2.49$, $p < .05$, $\eta p^2 = 0.027$ [0.000, 0.058]), Managed Service Provider (MSP)/Managed Security Service Provider (MSSP) ($F(4, 364) = 4.54$, $p < .05$, $\eta p^2 = 0.048$ [0.008, 0.089]), Local cyber security consultants ($F(4, 363) = 3.40$, $p < .05$, $\eta p^2 = 0.036$ [0.002, 0.072]), National Cyber Security Centre ($F(4, 366) = 2.75$, $p < .05$, $\eta p^2 = 0.029$ [0.000, 0.062]), and Police Cyber Alarm ($F(4, 364) = 3.09$, $p < .05$, $\eta p^2 = 0.033$ [0.001, 0.068]).

When analyzing organization type, there was a significant effect for General online searching (F(3, 367) = 2.75, $p < .05$, $\eta p^2 = 0.029$ [0.000, 0.062]) and Managed Service Provider (MSP)/Managed Security Service Provider (MSSP) (F(3, 365) = 3.96, $p < .05$, $\eta p^2 = 0.042$ [0.005, 0.080]).

When analyzing organization maturity, there was a significant effect for satisfaction with the information, advice or support received (F(4, 55) = 3.00, $p < .05$, $\eta p^2 = 0.179$ [0.000, 0.327]) and Managed Service Provider (MSP)/Managed Security Service Provider (MSSP) (F(4, 365) = 2.64, $p < .05$, $\eta p^2 = 0.028$ [0.000, 0.060]). Post-hoc Tukey test results reveal that Industry Leader organizations had a greater satisfaction score than all other organization maturity levels ($M = 4.60$, SD = 0.55), with a significantly higher satisfaction level than growth-stage startups ($M = 3.00$, SD = 1.16). Mature organizations ($M = 4.15$, SD = 0.86) also had a significantly higher satisfaction level than growth-stage startups ($M = 3.00$, SD = 1.16).

In relation to organization sector, there was a significant effect for the Information Technology sector for Cyber Aware (F(17, 351) = 1.81, $p < .05$, $\eta p^2 = 0.067$ [0.000, 0.088]), Cyber Essentials (F(17, 349) = 8.09, $p < .001$, $\eta p^2 = 0.245$ [0.148, 0.298]), ISO 27001 (F(17, 348) = 6.756, $p < .001$, $\eta p^2 = 0.214$ [0.118, 0.265]), Information Commissioner's Office guidance on SMEs (F(17, 349) = 2.36, $p < .05$, $\eta p^2 = 0.086$ [0.010, 0.114]), NCSC 10 steps to cyber security (F(17, 352) = 3.62, $p < .001$, $\eta p^2 = 0.126$ [0.040, 0.164]), NCSC board toolkit (F(17, 350) = 3.25, $p < .001$, $\eta p^2 = 0.115$ [0.031, 0.151]), NCSC small business guide (F(17, 349) = 3.14, $p < .001$, $\eta p^2 = 0.112$ [0.029, 0.147]), PCI Data Security Standard (DSS) (F(17, 350) = 4.29, $p < .001$, $\eta p^2 = 0.146$ [0.057, 0.188]), IASME Cyber Assurance (F(17, 348) = 6.69, $p < .001$, $\eta p^2 = 0.212$ [0.116, 0.263]), Managed Service Provider (MSP)/Managed Security Service Provider (MSSP) (F(17, 350) = 3.42, $p < .01$, $\eta p^2 = 0.120$ [0.036, 0.157]), Local cyber security consultants (F(17, 349) = 1.99, $p < .05$, $\eta p^2 = 0.074$ [0.002, 0.097]), Police Cyber Protect Officers (F(17, 349) = 2.74, $p < .001$, $\eta p^2 = 0.099$ [0.019, 0.130]), National Cyber Security Centre (F(17, 352) = 2.96, $p < .001$, $\eta p^2 = 0.105$ [0.024, 0.138]), Regional cyber resilience center (F(17, 349) = 2.81, $p < .001$, $\eta p^2 = 0.101$ [0.021, 0.133]), Regional cyber security cluster (F(17, 349) = 4.56, $p < .001$, $\eta p^2 = 0.155$ [0.064, 0.198]), Federation of small businesses (FSB) guidance (F(17, 349) = 2.65, $p < .001$, $\eta p^2 = 0.096$ [0.017, 0.127]) and Police Cyber Alarm (F(17, 350) = 2.10, $p < .05$, $\eta p^2 = 0.077$ [0.004, 0.102]).

Figure 4 shows six representative sectors: Construction, Manufacturing, Healthcare, Education, Retail and Information Technology. These sectors reflect different levels of engagement across five key support routes and illustrate the range

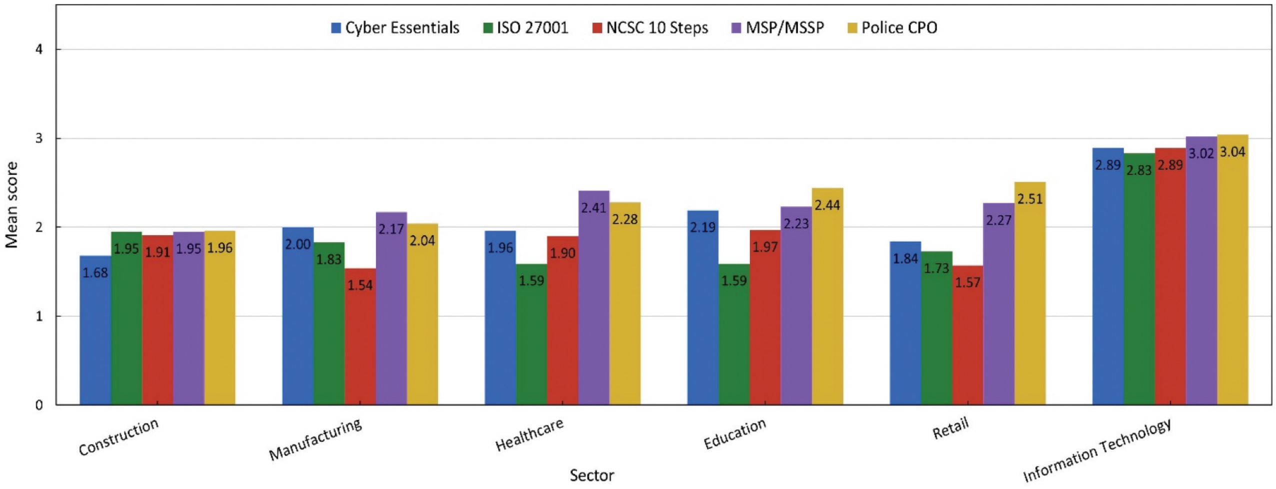

Figure 4. Mean awareness and use of five representative cyber security support routes by sector (means). The routes, cyber Essentials, ISO 27001, NCSC 10 steps to cyber security, MSP/MSSP, and Police cyber Protect Officers, each showed significant differences across at least one organisational category (see Table 8) and together represent government, industry and policing support. Across all sectors, Information Technology demonstrate the highest engagement across all routes.

Table 8. RQ3 one-way ANOVA results.

The extent to which the category of an SME varies in the support routes they take				
	Organisation Size			
Support route	**F**	**df**	**p**	**ηp^2 [95% CI]**
ISO 27001	3.461	4, 362	<0.01	0.037 [0.003, 0.074]
PCI Data Security Standard (DSS)	2.49	4, 364	<0.05	0.027 [0.000, 0.058]
Managed Service Provider (MSP)/Managed Security Service Provider (MSSP)	4.54	4, 364	<0.05	0.048 [0.008, 0.089]
Local cyber security consultants	3.40	4, 363	<0.05	0.036 [0.002, 0.072]
National Cyber Security Centre	2.75	4, 366	<0.05	0.029 [0.000, 0.062]
Police Cyber Alarm	3.09	4, 364	<0.05	0.033 [0.001, 0.068]
	Organisation type			
Support route	**F**	**Df**	**p**	**ηp^2 [95% CI]**
General online searching	2.75	3, 367	<0.05	0.029 [0.000, 0.062]
Managed Service Provider (MSP)/Managed Security Service Provider (MSSP)	3.96	3, 365	<0.05	0.042 [0.005, 0.080]
	Maturity of organisation			
Support route	**F**	**Df**	**p**	**ηp^2 [95% CI]**
Satisfaction with the information, advice or support received	3.00	4, 55	<0.05	0.179 [0.000, 0.327]
Managed Service Provider (MSP)/Managed Security Service Provider (MSSP)	2.64	4, 365	<0.05	0.028 [0.000, 0.060]
	Sector of organisation			
Support route	**F**	**Df**	**p**	**ηp^2 [95% CI]**
Cyber aware	1.81	17, 351	<0.05	0.067 [0.000, 0.088]
Cyber essentials	8.09	17, 349	<0.001	0.245 [0.148, 0.298]
ISO 27001	6.756	17, 348	<0.001	0.214 [0.118, 0.265]
Information commissioner's office guidance on SMEs	2.36	17, 349	<0.05	0.086 [0.010, 0.114]
NCSC 10 steps to cyber security	3.62	17, 352	<0.001	0.126 [0.040, 0.164]
NCSC board toolkit	3.25	17, 350	<0.001	0.115 [0.031, 0.151]
NCSC small business guide	3.14	17, 349	<0.001	0.112 [0.029, 0.147]
PCI data security standard (DSS)	4.29	17, 350	<0.001	0.146 [0.057, 0.188]
IASME Cyber Assurance	6.69	17, 348	<0.001	0.212 [0.116, 0.263]
Managed Service Provider (MSP)/Managed Security Service Provider (MSSP)	3.42	17, 350	<0.01	0.120 [0.036, 0.157]
Local cyber security consultants	1.99	17, 349	<0.05	0.074 [0.002, 0.097]
Police cyber protect officers	2.74	17, 349	<0.001	0.099 [0.019, 0.130]
National cyber security centre	2.96	17, 352	<0.001	0.105 [0.024, 0.138]
Regional cyber resilience centre	2.81	17, 349	<0.001	0.101 [0.021, 0.133]
Regional cyber security cluster	4.56	17, 349	<0.001	0.155 [0.064, 0.198]
Federation of small business (FSB) guidance	2.65	17, 349	<0.001	0.096 [0.017, 0.127]
Police cyber alarm	2.10	17, 350	<0.05	0.077 [0.004, 0.102]

of behaviors observed in the data. Information Technology shows the highest overall engagement.

In addition to the separate one-way analyses, multivariable general linear models were estimated for each support route outcome to examine the independent contribution of organizational size, maturity and sector when entered simultaneously. Effects were evaluated using Type II sums-of-squares F-tests, allowing each predictor to be assessed while adjusting for the others. Given the number of support routes examined, *p*-values were adjusted using the Benjamini – Hochberg false discovery rate (FDR) procedure (q = .05). Full model statistics, including F-tests, FDR-adjusted *p*-values and effect sizes (ηp^2), are reported in Table 9.

When organizational size, maturity and sector were analyzed simultaneously, sector emerged as the most consistent independent predictor of engagement with formal standards and institutional support routes. After FDR correction, significant sector effects were observed for Cyber Essentials ($\eta p^2 = .131$), ISO 27001 ($\eta p^2 = .133$), Information Commissioner's Office guidance ($\eta p^2 = .092$), the National Cyber Security Centre 10 Steps to Cyber Security ($\eta p^2 = .138$), the National Cyber Security Center Board Toolkit ($\eta p^2 = .122$), the National Cyber Security Center Small Business Guide ($\eta p^2 = .153$), PCI Data Security Standard ($\eta p^2 = .181$), IASME Cyber Assurance ($\eta p^2 = .168$), Police Cyber Protect Officers ($\eta p^2 = .097$), the National Cyber Security Center ($\eta p^2 = .099$), Regional Cyber Resilience Centres ($\eta p^2 = .115$), Regional Cyber Security Clusters ($\eta p^2 = .129$), Federation of Small Businesses guidance ($\eta p^2 = .097$), and Police Cyber Alarm ($\eta p^2 = .102$). Sector effects were generally small-to-moderate in magnitude, with comparatively larger effects observed for PCI DSS ($\eta p^2 = .181$), IASME Cyber Assurance ($\eta p^2 = .168$), and the NCSC Small Business Guide ($\eta p^2 = .153$). This pattern indicates that sectoral context plays a substantive role in shaping engagement with

Table 9. RQ3 multivariable results.

Multivariable predictors of support routes

Outcome	Predictor	F(df1, df2)	p	p(FDR)	ηp^2
Satisfaction	Size	1.18 (4, 55)	.336	.435	.113
	Maturity	2.03 (4, 55)	.110	.205	.180
	Sector	1.18 (14, 55)	.333	.435	.308
Cyber Aware	Size	3.22 (4, 345)	.013	.045	.036
	Maturity	1.84 (4, 345)	.121	.209	.021
	Sector	1.04 (17, 345)	.413	.500	.049
Cyber Essentials	Size	2.01 (4, 343)	.092	.180	.023
	Maturity	1.33 (4, 343)	.259	.367	.015
	Sector	3.05 (17, 343)	<.001	<.001	.131
ISO 27001	Size	2.57 (4, 342)	.038	.101	.029
	Maturity	0.23 (4, 342)	.919	.923	.003
	Sector	3.08 (17, 342)	<.001	<.001	.133
Information Commissioner's Office guidance on SMEs	Size	3.11 (4, 343)	.016	.049	.035
	Maturity	2.01 (4, 343)	.093	.180	.023
	Sector	2.04 (17, 343)	.009	.032	.092
National Cyber Security Centre 10 Steps to Cyber Security	Size	2.16 (4, 346)	.073	.162	.024
	Maturity	3.16 (4, 346)	.014	.047	.035
	Sector	3.27 (17, 346)	<.001	<.001	.138
National Cyber Security Centre Board Toolkit	Size	3.80 (4, 344)	.005	.021	.042
	Maturity	1.63 (4, 344)	.165	.271	.019
	Sector	2.82 (17, 344)	<.001	.002	.122
National Cyber Security Centre Small Business Guide	Size	1.32 (4, 343)	.261	.367	.015
	Maturity	0.23 (4, 343)	.923	.923	.003
	Sector	3.65 (17, 343)	<.001	<.001	.153
PCI Data Security Standard (DSS)	Size	4.63 (4, 344)	.001	.007	.051
	Maturity	2.26 (4, 344)	.062	.144	.026
	Sector	4.46 (17, 344)	<.001	<.001	.181
IASME Cyber Assurance	Size	2.45 (4, 342)	.046	.117	.028
	Maturity	1.29 (4, 342)	.273	.370	.015
	Sector	4.06 (17, 342)	<.001	<.001	.168
General online searching	Size	1.13 (4, 347)	.340	.435	.013
	Maturity	0.92 (4, 347)	.455	.515	.010
	Sector	1.03 (17, 347)	.423	.502	.048
Managed Service Provider (MSP)/Managed Security Service Provider (MSSP)	Size	4.89 (4, 344)	<.001	.005	.054
	Maturity	2.91 (4, 344)	.022	.063	.033
	Sector	1.44 (17, 344)	.117	.206	.066
Local cyber security consultants	Size	2.32 (4, 343)	.057	.135	.026
	Maturity	0.56 (4, 343)	.691	.741	.007
	Sector	1.90 (17, 343)	.017	.052	.086
Police Cyber Protect Officers	Size	3.97 (4, 343)	.004	.018	.044
	Maturity	0.31 (4, 343)	.871	.897	.004
	Sector	2.16 (17, 343)	.005	.021	.097
National Cyber Security Centre	Size	1.65 (4, 346)	.162	.271	.019
	Maturity	0.99 (4, 346)	.411	.500	.011
	Sector	2.24 (17, 346)	.003	.018	.099
Regional Cyber Resilience Centre	Size	2.11 (4, 343)	.079	.170	.024
	Maturity	0.69 (4, 343)	.600	.657	.008
	Sector	2.63 (17, 343)	<.001	.004	.115
Regional Cyber Security Cluster	Size	2.05 (4, 343)	.087	.180	.023
	Maturity	1.10 (4, 343)	.357	.448	.013
	Sector	2.98 (17, 343)	<.001	<.001	.129
Federation of Small Businesses (FSB) guidance	Size	1.31 (4, 343)	.266	.367	.015
	Maturity	0.77 (4, 343)	.543	.604	.009
	Sector	2.16 (17, 343)	.005	.021	.097
Police Cyber Alarm	Size	1.42 (4, 344)	.228	.349	.016
	Maturity	1.33 (4, 344)	.257	.367	.015
	Sector	2.31 (17, 344)	.002	.014	.102

certification schemes, regulatory frameworks and structured institutional guidance. Sector did not retain independent associations with Cyber Aware, general online searching, managed service providers, local consultants, or satisfaction after FDR correction.

Organizational size demonstrated more selective independent associations following adjustment and FDR correction. Significant size effects were observed for Cyber Aware ($\eta p^2 = .036$), Information Commissioner's Office guidance ($\eta p^2 = .035$), the National Cyber Security Centre

Board Toolkit ($\eta p^2 = .042$), PCI Data Security Standard ($\eta p^2 = .051$), Managed Service Providers or Managed Security Service Providers ($\eta p^2 = .054$), and Police Cyber Protect Officers ($\eta p^2 = .044$). These effects were small in magnitude overall, with comparatively larger effects observed for engagement with managed service providers and PCI DSS. This suggests that organizational scale may be particularly relevant for outsourcing security services and engaging with compliance-oriented standards, while playing a more limited role in other guidance routes once sector is taken into account.

In contrast, organizational maturity demonstrated limited independent effects once size and sector were included in the model. Following FDR correction, maturity retained a statistically significant association only with use of the National Cyber Security Centre 10 Steps to Cyber Security ($\eta p^2 = .035$). All other maturity effects were reduced to non-significance. This indicates that maturity may be specifically related to engagement with structured strategic guidance, but does not independently predict broader uptake of certification schemes, advisory bodies or regional support mechanisms once organizational size and sectoral composition are controlled.

No independent effects of size, maturity or sector were observed for satisfaction following FDR correction, suggesting that overall satisfaction with support routes does not vary systematically across organizational categories once these structural characteristics are accounted for.

Overall, the multivariable results indicate that variation in engagement with support routes is structured predominantly by sector, with organizational size contributing modestly to engagement with compliance-based standards and outsourced services, and organizational maturity playing a more limited and route-specific role.

4.4. *RQ4. What are the factors that influence whether SMEs access resources to reduce their cyber security risk?*

To answer RQ4, a Thematic Analysis was conducted on the follow-up semi-structured interviews. A total of 33 general codes (e.g. "support lacks relevance for SME") emerged from the interview transcripts representing the factors that influence whether SMEs access resources to reduce their cyber security risk. The general codes were combined into 12 lower-order themes across seven higher-order themes. The list of themes can be found in Table 10. The themes comprised: "Limited awareness of available support" (with the sub-themes of "Lack of awareness of risks" and "Minimal awareness of where to seek support"); "Underestimate risks" (with the sub-themes "The influence of previous attacks," and "Bias towards own capability"); "Resource constraints" (with the sub-themes "Financial" and "Competing priorities"); "Support requirements" (with the sub-themes "Relevance" and "Communities"); "Expectations from cyber security providers" (with the sub-themes "Perceptions of small businesses" and "Sales shows"); "Lack of relevant support" and "Simple messaging" (with the sub-themes "Governmental resource" and "Case studies provide meaning").

4.4.1. *Limited awareness of available support*

4.4.1.1. Lack of awareness of risks. Throughout the discussions, only one SME provided evidence that

Table 10. List of higher and lower order themes.

Higher-order themes	Lower-order themes
Limited awareness of available support	Lack of awareness of risks Minimal awareness of where to seek support
Underestimate risks	The influence of previous attacks Bias towards own capability
Resource constraints	Financial Competing priorities
Support requirements	Relevance Communities
Expectations from cyber security providers	Perceptions of small businesses Sales shows
Lack of relevant support	
Simple messaging	Governmental resource Case studies provide meaning

they knew about the risks and threats that could affect their organization. This in turn affected how aware they were of available support. One participant, who had a background in data protection, implied that this lack of awareness was evident in their organization:

> One of the things that I (am) trying to get across to the people in our organisation, particularly those are on the committee is that it's not just about making sure that your particular society email account hasn't been hacked. It's about all the other email accounts that you'll have (Participant 10)

Another participant, who is an SME in the IT sector, noted that SMEs can struggle with a basic understanding of the risks, perhaps because they do not "live and breathe" cyber security. This is evident in the following Participant who also described SMEs struggling with the basics of cyber security:

> I am on because a lot of clients, they do try their best but they don't live and breathe this language or terminology or in this space they really struggle sometimes with some of the basics (Participant 2)

For SME owners who do not understand the risks and the threats that apply to them, it can become something of a negative to them in knowing where to go for support. As the following participant described, this can also become "quite fatiguing":

> I think it can be quite fatiguing for, you know, especially for any individual who's running the business, who just doesn't really get it (Participant 4)

Taken together, these accounts suggest that limited understanding of cyber security risks may reduce the perceived urgency to seek external support. Where threats are not clearly recognized or are experienced as complex and cognitively demanding, engagement with available guidance is less likely to occur proactively.

4.4.1.2. Minimal awareness of where to seek support. Seven participants described not knowing where to seek support, with some defaulting to an I.T provider they have worked with before. The difficulty of knowing where to seek trustworthy targeted support was evident for some SMEs, as reflected in one participant's account:

> I think there's a lot where, from my perspective, you just need something targeted (but) 'Where the heck do I get support? How do I do it?' (Participant 1)

When participants were not sure where to go for support or advice, their first stop may be to do a search online. As identified by the following participant, they may default to either the ICO's website or to Google:

> I didn't find the information I wanted, maybe I'd go on the ICO's website or I'd go on Google (Participant 11)

For SMEs who wanted to seek expert advice, either online or from a provider, the challenge was often simply navigating the available options and applying them to their own organization. This uncertainty was reflected in the experience of the following participant:

> If you research something on the Internet, you get different variations of the same answer and it's always difficult to then think, 'How do I implement this within what I'm working on?' and that takes up a lot of time. (Participant 3)

These extracts indicate that uncertainty about where to begin, and difficulty identifying relevant and trustworthy sources, may act as practical barriers to engagement. Rather than reflecting a lack of interest, lower uptake of formal support may stem from navigational complexity and the challenge of translating general advice into actionable steps within the SME context.

4.4.2. Underestimate risks

4.4.2.1. The influence of previous attacks. Despite regular exposure to clear signs of cyber threats, some SMEs still believed they were unlikely to be affected. This underestimation of the cyber security risk, even when evidence of vulnerability was directly observable, was captured powerfully by one participant:

> I think what doesn't work, and it should, and I don't know why it doesn't, is the head-in-the-sand [attitude]. It's 'someone else, it's not going to affect me,' despite the statistics, despite the fact they will see phishing emails. I've tried to frighten people by taking long logs of people trying to brute-force attack their way into our system . . . it's minute by minute, all around the world . . . and people

> go, 'Oh yeah, it's really bad there,' and then do nothing about it. It's happening to someone else, it's not happening to me. (Participant 5)

The change in perception of cyber security risk was evident more for those SMEs who had an attack on their own organization. However, it was only after experiencing a cyber attack that they decided to have discussion with a provider about seeking cyber security support:

> We've started discussions about cyber security, but only as a consequence of us falling foul to some email spoofing, etc . . . so I'm not sure we would have started those discussions at this point in our growth and if that hadn't have happened (Participant 11)

One participant outlined that despite various organizations offering free support or advice, SMEs still do not take up this resource. Although this participant did not describe why this might have been the case, it may be probable that a lack of perceived exposure or previous experience of a cyber attack could be influencing this behavior:

> I've seen different initiatives from the National Cyber Security Centre or the Cyber Resilience centres around the UK who actually offer free services for SMEs and still SMEs will not engage, they will not actually, you know seek that support which is free (Participant 8)

These accounts suggest that perceived personal relevance of cyber security risk is a key driver of engagement. Where risk is underestimated, SMEs may be less likely to seek support proactively, even when indicators of threat are visible or when support is freely available. In contrast, direct experience of an incident appears to act as a trigger for action, indicating that support-seeking may often be reactive rather than preventative.

4.4.2.2. Bias toward own capability. Four participants appeared to take a favorable view to their own employees and their ability to combat a potential cyber threat. As the following participant openly described, their approach to whether to train their employees was influenced by their own perception of their employees:

> And in terms of how that sort of plays down into training here, I think there was a large amount of, I would say bias where I kind of perhaps projected in my mind that the people I employ, are smart people so they wouldn't click on a bad email (Participant 4)

There was also a perception that because employees may already be equipped with the skills and experience to handle cyber threats, that the organizations' approach to training and development would be different. As outlined by the following Participant, because employees had been in a corporate environment previously, there was an assumption that they would already have the required understanding within cyber security:

> The majority of our employees have worked in corporate environments before and they sort of understand the basic concept of cyber security (Participant 11)

These extracts indicate that some SMEs may take a favorable view of their own capability, which can reduce the perceived need for further training or external guidance. Where leaders assume that staff competence or prior experience is sufficient, investment in preventative support may be deprioritised, potentially limiting proactive engagement with available resources.

4.4.3. Resource constraints

4.4.3.1. Financial. Participants spoke about the difficulty in being able to afford cyber security support, that, despite recognizing potential financial gains from this expenditure, they felt it was not worthwhile for them:

> Funding wise I can only do the free ones. You know when they're saying it's sort of £50 a year. No. Am I going to get any business from that? No (Participant 1)

Whilst participants were not overly sure on where to find a cyber security provider, their perception was that it would cost them a large amount, and with no guarantee of the outcome, this created a hesitation about whether to get advice from such an organization as one participant described the general views of SMEs:

> Nobody gives a damn. It's too expensive. It's all a waste of money. Why should they bother? They won't get hacked because they're a small company. (Participant 6)

These accounts highlight how cost sensitivity and uncertainty about return on investment shape decision-making in SMEs. Where cyber security expenditure is viewed as speculative rather than immediately beneficial, organizations may defer or avoid engagement with external support, particularly where budgets are tightly constrained.

4.4.3.2. Competing priorities. Participants also noted that it was difficult to prioritize cyber security support when they have a number of other competing areas that they could spend the money on. Six SMEs spoke about having many different activities to be completed at the same time and that cyber security often falls down the priority list. This was particularly identified within very small SMEs:

> The problem is that we don't have the financial capital to get any sort of external advice on these things and if we did, it would be, you know, #100 on the list of things we need to do and get and get money on. and that's what makes it quite difficult for particularly really small businesses . . . and it's also what makes us very vulnerable (Participant 11)

Focusing time on the main aspect of their business was difficult to override when thinking about utilizing cyber security support and this was despite them recognizing the importance of cyber security for their business. For example, the following participant who works in Audiology, described potentially choosing an Audiology conference over a cyber security conference given their limited budget:

> Again, there's a limited budget. There are things that you think, no, I really ought to do this, but if you were saying right pay for a British Academy, British Academy of Audiology conference versus a cyber security conference, I'd probably go more for the audiology and the business (Participant 1)

In this context, cyber security competes with core business activities for limited time and financial resources. Even where its importance is acknowledged, competing operational demands may displace preventative action, contributing to delayed engagement with support and increasing organizational vulnerability.

4.4.4. Support requirements

4.4.4.1. Relevance. Participants' perception of cyber security support was that it needed to involve someone that understood their organization and their environment. Such an understanding would ensure the provider was able to give a more effective service, could work quickly and could understand the issues that the SME faced. Some participants said that they found it difficult to identify such providers but as described by the following provider, did recognize that this understanding and knowledge would be a beneficial asset if they could find a provider with it:

> And so for us, having somebody, even it was if it was somebody that understood our environment that could help us really quickly if we had an issue . . . and that it would almost be an extension or an extension of me type of thing, but somebody with the knowledge to do that to make those changes, that would help us immensely (Participant 3)

Additionally, some participants felt that it would be helpful to have support that was based on the size of their organization to ensure it was tailored to them which would enable to support and advice to be relevant, specific and personal to the SME. There was a general thought amongst SMEs that some providers were more catered for specific sizes of SMEs than others, and that finding a provider with specific advice based on the size of the business would be beneficial:

> What I would like (is) really specific advice based on the size of our business, meaning the amount of capital you're probably going to be able to spend on these sort of things and a lot of the advice out there (should be) very personal advice (Participant 11)

These extracts point to the importance of contextual fit in shaping engagement with cyber security support. Where guidance is perceived as generic or insufficiently tailored to organizational size, sector or capability, it may be regarded as less actionable. In contrast, support that reflects the specific operating environment of the SME appears more likely to be viewed as valuable and worth pursuing.

4.4.4.2. Communities of support. Finding communities of support was deemed as a valuable exercise for some participants, particularly to help build a network. However, finding these communities of support was also something they found difficult to do because they were not aware of other SMEs they could build a community of support with. This was emphasized by the following Participant who found it difficult to build a community due to their location:

> What we don't know of, and I know it was one of the things that they also say you should do, is have a network of people that you can share best practice

> with . . . But there's nobody around. I mean, we're based in a small town, there are hardly any other companies (here) (Participant 9)

For participants who do not have a technical background in Information Technology, it appeared that they were not sure where to find communities despite actively searching for them:

> I think one of the things I've struggled to find is like a community really. I mean, I've looked. I've looked in various places and I think because my role isn't necessarily deeply technical, it, you know, it's more strategic, it has been difficult to do (Participant 7)

The difficulty in identifying peer networks suggests that access to informal communities may influence how SMEs learn about and engage with cyber security practices. Where such networks are absent or difficult to access, opportunities for shared learning and trusted recommendation of support routes may be limited, potentially reducing confidence in taking preventative action.

4.4.5. Expectations from cyber security providers

4.4.5.1. Perceptions of small businesses. Some participants had a view that many providers were not actively looking to support SMEs, perhaps due to the lack of financial resource these organizations potentially have compared to larger organizations:

> So traders and that kind of marketplace, when you start going to your bigger organisations, they probably won't want to know because you're too small. They won't make enough money out of you (Participant 1)

One participant spoke about the requirements from external providers, such as to be certified in cyber security essentials. This participant implied that the provider organization had not taken the small organizations' needs and requirements into account, given the small size of the organization:

> They might require me to get certified with cyber security essentials, which I don't know very much about. Having a quick look at it looks quite onerous for an organisation like mine, which is basically tiny (Participant 12)

This viewpoint was also observed in another participant, who outlined that the provider organization had not understood the requirements of the SME:

> Although the other was pushing it fine, we came back (they said) we can have 50 items for 80 odd quid. Well, I haven't got 50 items (Participant 1)

These accounts suggest that perceived misalignment between provider models and SME realities may discourage engagement with external support. Where guidance or certification requirements are experienced as burdensome, overly standardized or oriented toward larger organizations, smaller SMEs may be less inclined to pursue these formal schemes, such as Cyber Essentials.

4.4.5.2. Sales shows. Participants were also wary of providers who were looking to sell products and services, and believed that as such the offering was perhaps not always in the SMEs interests. This has made some SMEs wary of some providers and as described the following Participant, taking some of their sales advice with a "pinch of salt":

> Most of the stuff that come up on the first page is from people trying to sell you stuff . . . so you always kind of have to take it with a bit of a pinch of salt. It's not necessarily that independent (Participant 12)

Similarly, another participant outlined that they were looking for a value conversation when they go to IT events and providers are instead looking to sell their products. As such, there can often be a disconnect between what the provider is looking for at a Sales show compared to the value an SME is looking for from the provider at that time:

> That's the hardest part in IT is that you go to these events and ultimately people are there to try and sell you something and actually having a conversation and understanding other people's challenges and then bringing them back to your businesses, it's more of a value conversation for me (that I want) (Participant 7)

This reservation was also felt when participants spoke about looking for resources online, and felt it was a challenge to find the relevant resources without the potential sale of products and services. Some SMEs described having follow up communications from providers who were then looking to sell irrelevant services after the SME had sought cyber security material to support them:

> If I go on Google Top 10 tips for cyber security, I'm going to have one of the major players throwing content

> at me trying to guide me into a funnel to go and buy some software or some hardware (Participant 4)

Expressions of skepticism toward commercially driven advice indicated that trust plays a central role in shaping engagement. When support is perceived primarily as a sales opportunity rather than a source of independent guidance, SMEs may disengage or rely on informal alternatives, potentially limiting their exposure to structured or evidence-based resources.

4.4.6. Lack of relevant support

In terms of value and effectiveness of cyber security support, many participants spoke about the generic nature of support, with the challenge of finding support that is relevant to their organization:

> I think that there is a challenge when I look for this information, to find the information that is probably more relevant to my stage of business and or competency (Participant 4)

One participant who had worked with a provider felt that the results of the service were "questionable," partly due to the provider not taking into account the specific nature of the SME:

> Where we have done it, which we have, I've had questionable results as well. You know, they've not really listened to the brief and not taken into the contacts, the type of organisation that we are (Participant 5)

Another participant spoke about being provided cyber security refresher training from their clients. Whilst they found this useful, the participant found the training to be basic and not specific enough for them:

> I've done general awareness security training for whoever my employer role client has been. They are a good refresher, and sometimes they have a different perspective on things and can be quite helpful, but generally I find those kind of things to be a bit too basic and not to be specific enough (Participant 12)

These accounts indicate that perceived lack of relevance may weaken the practical impact of cyber security support. When guidance or training is experienced as too generic, insufficiently tailored, or misaligned with organizational context, SMEs may question its value and be less likely to engage further. In this way, relevance appears to influence not only initial uptake, but also continued use and implementation of recommended practices.

4.4.7. Simple messaging

4.4.7.1. Governmental resource.

Many participants were aware of and spoke favorably about the National Cyber Security Centre (NCSC). The NCSC was one of a few organizations where participants were positive about the resources provided, and are resources they would go back to:

> Yeah, I mean, obviously the NCSC, they are really, really good. I feel like particularly in the period where I've been concentrating so much on the cyber that they have like grown as an organisation and (their resource) really helps. I use their resources quite a lot (Participant 7)

One participant highlighted that the reason they returned to the NCSC resource was because it was "easy to understand":

> We use a lot of the stuff on the NCSC website for guidance. That's not necessarily reaching out (to them for) their stuff. It's actually really, really good … we found we did find it easy to understand (Participant 9)

Another participant spoke positively about the practical resources on the NCSC website, such as the templates provided. They also described a favorable experience on a workshop hosted by the NCSC:

> You know, there are a lot of the templates they have on the website, a lot of the guidance, I was on an SME workshop they were doing on Monday lunchtime, they did like an hour session with SMEs which was great and was all that was what it was focused on (Participant 7)

Positive perceptions of the NCSC suggest that clarity, accessibility and practical tools may lower barriers to engagement. Where guidance is presented in a straightforward and SME-focused manner, it appears more likely to be trusted, revisited and incorporated into organizational practice.

4.4.7.2. Case studies provide meaning.

Case studies were highlighted by participants to be an important resource to help SMEs, for example the following participant outlined that it could be important for case studies to describe examples of where cyber security has not gone well:

> . . . having some really good case studies and really good understandings of where specifically in the SME market this has gone terribly wrong . . . and this could happen to you and this is why. I think that would help get people in the room (Participant 11)

Case studies were identified as a good starting point resource for SMEs, to help show how they have been affected and the direct consequence on the organization:

> I can only speak from personal experience and the reason that we've got better at it is because we've seen first hand the effect it can have on other companies, so that's probably a good place to start, case studies about people that have been directly affected and what's happened to their business (Participant 8)

The emphasis on case studies indicates that concrete and relatable examples may increase the salience of cyber security risks. By illustrating tangible consequences for similar organizations, such examples appear to strengthen perceived relevance and may encourage more proactive consideration of support and preventative measures.

5. Discussion

This study analyzed SME survey responses to examine whether the 1) types of controls implemented, 2) levels of cyber security awareness, knowledge, attitude and culture, and 3) patterns of support use differ across SME categories (i.e. size, type, maturity and sector). Follow-up interviews were also conducted with SMEs to understand the factors that influence SMEs in accessing resources to reduce their cyber security risk. Studies show that most SMEs may not have enough cyber security measures in place and have a full comprehension of what needs to be done to maintain strong cyber security. Qualitative observations indicate that many SMEs underestimate their susceptibility to cyber security threats, face competing objectives or resource constraints that hinder action, and lack clarity regarding the appropriate sources of support.

The results show that SMEs behave differently when it comes to cyber security, particularly depending on the industry in which they operate, with organizational size also contributing to variation in governance and capability outcomes. Most SMEs in the sample appear to not have the basic skills they need to handle cyber risks well. To understand these results, effect sizes (ηp^2) and their 95% confidence intervals along with *p*-values were analyzed to understand both the magnitude and precision of observed differences. Within the analyses, the majority of effects were modest in their magnitude. This pattern is consistent with broader cyber security behavioral research, where empirical reviews of user-focused security studies indicate that many reported effects are small-to-moderate and that large effects are comparatively rare (e.g., Groß, 2021). Importantly, while sector effects were often larger in magnitude, multivariable analysis indicated that many maturity effects observed in unadjusted analyses were attenuated once organizational size and sector were accounted for. Maturity retained more selective associations, particularly with concern about cyber security, rather than broad implementation differences. Across all three quantitative research questions (RQ1-RQ3), sector emerged as the most consistent independent predictor of cyber security behavior once organizational characteristics were analyzed simultaneously. Even after false discovery rate correction, sector effects remained statistically robust and were frequently larger in magnitude than those associated with size or maturity.

Across all research questions, the role of organizational maturity was less prominent than sector but was still theoretically meaningful. In line with maturity-model approaches, developmental stage reflects the extent to which organizational routines and governance structures have become institutionalized. While multivariable analyses indicate that many maturity effects weaken once sector and size are controlled, the persistence of associations with concern and selected governance-oriented controls suggests that developmental stage captures differences in organizational formalization, which reinforces the interpretation of maturity as a relevant developmental indicator.

5.1. Organization category

When analyzing organization category on controls implemented, it was perhaps unsurprising that sole traders had a lower amount of regular training and awareness programmes than other organization sizes. Previous research has identified a misconception that SMEs often believe that cyber threats primarily impact larger organizations (Manzoor et al., 2024), and it could be that sole traders do not undertake regular training and awareness programmes given this misconception. As a result, sole traders may feel that the additional expense of awareness and training programmes is not worth it. The Cost–Benefit Analysis Theory from psychology and behavioral economics could explain this behavior (Kesswani & Kumar, 2015). According to this theory, individuals weigh the perceived costs and benefits of a decision before taking action. In this case, sole traders may perceive the cost of awareness and training programs (in terms of time, money, or effort) as outweighing the benefits they expect to receive, even if those benefits include potential financial gains. This finding could potentially be explained by Prospect Theory, which suggests that individuals may prioritize loss avoidance over equivalent gains (Kahneman & Tversky, 1979). Sole traders may view the expenditure as an immediate loss, overlooking the prospective long-term financial advantages and resulting in their reluctance to invest in such programmes.

Self-Determination Theory (SDT) may also explain the behavior if it results from a decrease in intrinsic motivation (Ryan & Deci, 2000). SDT differentiates between extrinsic and intrinsic motivation, suggesting that motivation is more likely to be maintained when the needs for autonomy, competence, and relatedness are satisfied. As a result, some SMEs may only have concerns about cyber security when they feel they need to, such as when they have to follow rules, meet third party needs, or to become certified. These behaviors, influenced by external factors, may lead to temporary conformity rather than lasting engagement. On the other hand, SMEs are more likely to be engaged in cyber security when they have internalized the motivation, such as within their goals or values. Ensuring SMEs can see cyber security as an important part of their values and self-efficacy may help them to adopt cyber security practices even when they do not have to.

Industry Leading (i.e. those that see themselves as one of the most effective in their industry) organizations had a significantly higher cyber security training and awareness programmes to employees than all other organizations in the one-way analysis. It is possible that this is reflective of their overall culture as an organization i.e. as an industry leader in their field, they also have the general cultural mind-set to be leading in other areas that are non-specific to their core business, such as cyber security. This may also be a factor in explaining why Industry Leading organizations have a greater level of formal policy or policies covering cyber security risks than other organizations and a business continuity plan covering cyber security risks compared to other organizations in the unadjusted analysis. Alternatively, it could be that such organizations believe they have a greater need to protect their data and assets and are therefore keen to invest in this area. However, when organizational size and sector were entered simultaneously in the multivariable models, several of these maturity effects were reduced, suggesting that some differences attributed to developmental stage may partly reflect sectoral positioning or organizational resource capacity rather than maturity alone. This pattern suggests that some maturity gradients identified in unadjusted analyses may reflect differences in sectoral context and organizational resources, rather than developmental stage alone. Future research is warranted to understand why Industry Leaders implement these sets of controls above and beyond other maturities of organizations (such as growth-stage startups). Interestingly, in the exploration of research question 2, Industry Leading organizations had a greater concern about cyber security and a greater interest in addressing cyber security issues than other organizations. These factors may help explain why Industry Leading organizations reported greater levels of controls in the unadjusted analyses. What is currently less clear is why Industry Leading organizations have a higher concern for cyber security and a greater interest in addressing cyber security issues than other organizations. Future research would benefit from exploring these areas, to understand the factors that influence Industry Leading organizational behavior.

The differences observed across organizational maturity categories can be interpreted using maturity-model approaches that conceptualize capability development as increased formalization and institutionalization of organizational routines.

Staged maturity approaches (e.g., CMMI-style) and governance-oriented approaches (e.g., COBIT) both treat maturity as progression toward more defined processes, clearer accountability, and more systematic oversight. In the present study, organizational maturity was operationalized as an organizational developmental stage. As such, the maturity findings are best interpreted as reflecting variation in the extent to which governance and routines may be established across SMEs, rather than as an appraisal of maturity model levels.

5.2. Awareness and knowledge

It is perhaps expected that Information Technology organizations display greater awareness and knowledge of cyber security practices as demonstrated in this study. These organizations also display strong cultural scores toward cyber security, such as an interest and concern for it compared to organizations in other sectors. Cyber security is seen as a priority by the top manager/owner in these organizations and employees in these organizations are trained in areas, such as phishing. This finding may reinforce the previous literature that awareness and knowledge, whilst not solely responsible for proactive cyber security behavior, are a key foundation toward attaining it (Gundu, 2019). The multivariable analyses reinforce this pattern, demonstrating that sector remained the strongest and most consistent predictor of awareness, knowledge, attitude and culture outcomes after adjusting for organizational size and maturity. It was also clear to see that early-stage startups have not implemented formal policies that cover cyber security risks or a business continuity plan addressing cyber security. This may be a reflection of where their priority lies (i.e. they may have a primary focus on other areas such as growing the organization over other activities, such as cyber security). Interventions to support early-stage startups in developing key documentation such as cyber security policies and continuity plans are therefore justified.

5.3. SME size and type

It is worth noting that while organizational size did not uniformly predict all cyber security outcomes, the multivariable analyses demonstrated that size retained independent associations with several governance-oriented controls (e.g., formal policies and a business continuity plan that covers cyber security), training provision, and perceived capability. This suggests that organizational scale may provide greater structural and resource capacity to formalize and support cyber security activities, even if size alone does not fully determine overall cyber security posture. It could be that given the heterogeneity of SMEs, size and type are not specific enough factors that define the category of an SME (i.e. there is too much heterogeneity within the size and type of an SME). It is perhaps notable that size did not uniformly influence all cyber security outcomes, despite retaining independent associations with governance and capability-related measures. It is possible that as an SME increases in size, there are more human resources dedicated to general I.T (e.g., by appointing an I.T Manager) than would be seen in smaller or micro-organizations. However, these larger SMEs did not appear to have any greater awareness and knowledge of cyber security best practices or the most appropriate support routes for their organization. Additionally, they did not appear to have the cultural factors that are important to reducing the cyber security risk of their organization, such as a concern or interest in addressing it. This pattern is consistent with previous work (e.g. Lee & Larsen, 2009), who also found that SME size did not significantly influence cyber security behavior but that factors, such as perceived severity, vulnerability and response efficacy were stronger predictors of adoption. Previous research has also observed that the day-to-day operational focus of SMEs constrains their ability to formulate an information security strategy, a pattern that appeared to be independent of organizational size (Gupta & Hammond, 2005). The present findings extend previous findings by showing that while size alone is not a defining factor, other organizational characteristics such as maturity and sector appear to play a more meaningful role. Specifically, Information Technology organizations consistently demonstrated higher awareness, stronger cyber security culture, and greater implementation of controls, while Industry Leading organizations showed elevated engagement in the unadjusted analyses. This comparison reinforces that maturity and sector differences may provide a more nuanced understanding of SME heterogeneity in cyber security behavior than size alone.

Interpreting these findings within the context of ongoing SME digitization provides an additional perspective. As digital technologies become more embedded within SME operations, reliance on interconnected systems may increase exposure to cyber threats (M. F. Arroyabe, C. F. A. Arranz, J. C. Fernandez de Arroyabe, et al., 2024; Saeed et al., 2023). In this context, the variation in findings may reflect differences in organizational readiness to sustain secure digitalization rather than solely differences in compliance behavior. Frameworks linking digital transformation and cyber security emphasize that governance structures, formalized processes and continuous improvement practices are central to maintaining resilience within digital environments (Metin et al., 2024). The current findings therefore enhance understanding of the relationship between SME characteristics and preparation in increasingly digital SME environments.

5.4. Awareness of available support

The qualitative finding that SMEs lacked awareness of available support aligns with previous research which has explored barriers to cyber security investment amongst SMEs (Alahmari & Duncan, 2021). In the current study, participants explained that as a result they did not know where to go for support, often defaulting to an I.T provider they had used before or to do a search online. Thus, it appears that there needs to be greater signposting for SMEs and the communities they interact with to better understand where there might be resources that can support them.

While the quantitative results identified broad trends in awareness and engagement with cyber security support, the qualitative findings extended these patterns by revealing the mechanisms behind them. These insights provide practical and behavioral explanations for the statistical patterns observed, thereby strengthening the mixed-methods contribution of the study. The qualitative results enhance interpretive and policy significance by contextualizing the quantitative patterns and demonstrating the real-world factors influencing SME behavior. The qualitative themes identified in this study align with various barriers previously investigated in earlier research, such as limited awareness, competing priorities, and financial constraints. The importance of the thematic analysis lies in its illustration of how these barriers persist and interact within SMEs, influencing their engagement with cyber security support. The analysis contextualizes these barriers within the experiences and perspectives of SMEs, providing practical and contextual insights that explain and enhance the quantitative findings. The thematic analysis thus not only identifies the barriers of awareness and resource limitations but also emphasizes several enhancements to the current SME cyber security research. For example, SMEs showed a skepticism toward providers that were perhaps motivated solely from a commercial point of view, which was seen in the “sales shows” theme, outlining how increasing trust in SMEs may enhance their engagement with cyber security support.

Beyond reinforcing known barriers such as awareness and resource constraints, the thematic analysis also highlighted several refinements that add nuance to existing SME cyber security research. Earlier studies have mainly focused on resource limitations and awareness gaps, often assuming that clearer guidance or additional training will drive behavior change. SMEs’ skepticism toward commercially motivated providers, identified in the “sales shows” theme, shows how trust can influence engagement with cyber security support. Likewise, the themes of “case studies provide meaning” and “communities of support” show that SMEs may often respond more favorably to peer examples and shared learning than to prescriptive guidance or policy documents. Given that these findings indicate that social connection and trust can play a key role for cyber security engagement in SMEs, future initiatives designed for SMEs have the opportunity to take these factors into account in their design to enhance SME engagement.

5.5. Risk perception in SMEs

The current study identified that many SMEs in the sample underestimate risks, and that experience of having a cyber security attack has influenced how SMEs perceive risk. This finding aligns with recent qualitative research demonstrating that SMEs frequently deprioritise cyber risk due to competing operational pressures, reactive risk management approaches, and a perception that they are unlikely targets (Adriko & Nurse, 2026). The finding may have been a factor in why Industry Leading SMEs have a greater concern for cyber security and had formal documentation such as policies in place for cyber security. Industry Leading organizations have been established for a longer time than other SMEs and it may be that during this time there are factors that have developed their mind-set toward cyber security, for example having experienced a cyber attack. Future research would therefore benefit from understanding the relationship between longevity of SME and their risk perception toward cyber security. Within this study, it was also found that SMEs may take a biased view toward their own organization, for example that their own employees have the skills and experience to handle cyber threats. Employees within SMEs may have an overconfidence bias, where they may think they are more competent at something, know more, or have more control over a situation than they really do (Kahneman & Tversky, 1982). This theory could explain this finding. In this situation, SMEs may think that their employees have the skills and experience to deal with cyber threats, even though this confidence may not be valid. Future research would therefore benefit from exploring why some organizations may have such overconfidence and also explore ways in which this overconfidence could be reduced, given its likely negative impact on the organization. These qualitative findings therefore provide contextual insights that further understanding of the quantitative results and have helped explain the differences found in the survey findings.

5.6. Resource constraints

Aligned with previous research, resource constraints in the form of financial constraints (Pawar & Palivela, 2023) can be a hindrance for SMEs in adopting cyber security support. Heidt et al. (2019) similarly found that limited financial and human resources, together with a lack of formalized processes and managerial time, act as systemic constraints on SME investment in IT security. Their concept of a "security divide" between SMEs and large organizations helps explain why even motivated SMEs struggle to translate awareness into sustained protective action. It is clear that SMEs are weighing up the cost benefits of using such support and that SMEs need to see the financial benefit of investing in it. Further research is warranted to understand the types of organizations that do not undertake cyber security support due to competing priorities. For example, within this research study, early stage startups had little concern for cyber security compared to Industry Leading SMEs and it is potentially these early stage startups that are finding it difficult to prioritize cyber security to a level that they need to. The qualitative findings demonstrate that SMEs are clear in the type of resources that they believe they would benefit from, specifically identifying the need for support that is relevant to them rather than generic in nature. Although SMEs are similar in some aspects (e.g. size) they differ in other aspects (e.g. maturity and sector) and it is therefore particularly pertinent for cyber security providers to ensure they are delivering resources and services that align to their wants and needs. Such interventions that SMEs described that could be useful related to finding communities of support, although participants did not know where to go to join or find a community of support.

5.7. Implications

This study has a number of implications for policy and practice. As highlighted in the literature review of this paper, over half of small organizations and at least 67% of medium-sized organizations report they have identified breaches or attacks in the last

12 months (DSIT, 2025). It is therefore vital that such organizations are equipped to reduce their risk of being impacted by a cyber breach or attack. This study has identified that it is Industry Leading and Information Technology organizations that are implementing the appropriate cyber security controls, have a high awareness, attitude, knowledge and culture toward cyber security and know which support routes are available. It is perhaps unsurprising that such organizations have demonstrated this behavior, and thus there are implications for cyber security organizations such as the National Cyber Security Centre (NCSC) in the UK to support organizations that do not sit within these category of organization. Not only can the NCSC outline the pressing need for these organizations to be doing more in relation to cyber security, but they can also recommend how such organizations could improve their cyber security based on the findings of this research study. They can also inform cyber security providers of the need to ensure that appropriate support is delivered in a way that would suit an SME (e.g. that it is specific and relevant) and in a form that would engage the SME population (e.g. in the form of communities if support).

Many SMEs also reported uncertainty about where to seek support or advice on cyber security and spoke about the financial pressure of adopting such security. This uncertainty was particularly evident among smaller organizations that lack dedicated I.T or security staff and often rely on informal sources of advice. These findings highlight a continuing need for practical initiatives that are accessible and low-cost for SMEs. Building on this, future work should include dissemination sessions designed to share freely available cyber security resources and examples of good practice tailored to SMEs, helping organizations identify trusted sources of information and take proportionate, affordable steps to strengthen their cyber security. In addition, there is clear value in developing targeted awareness and basic training sessions on cyber security that are tailored to the circumstances and capacities of SMEs. Such sessions could focus on the most common vulnerabilities identified in this and previous research, providing simple, actionable steps that can be implemented with limited technical expertise or financial investment. Delivering training in this way would help build confidence among SME owners and staff, encourage more consistent security practices and strengthen the overall resilience of smaller organizations.

5.8. Strengths and limitations

The current study has a number of strengths. Most notably, it explored differences across SME characteristics (i.e. size, type, maturity and sector) in areas such as 1) controls implemented, 2) levels of awareness, knowledge, attitude, and culture, and 3) the support routes SMEs use. This is the first study that has looked at such variables and thus has found some novel findings. Second, the study used a mixed-methods approach, integrating quantitative survey analysis with qualitative interview analysis. One main advantage of this approach was the ability to explain some of the findings identified within the survey results through the qualitative interviews. Third, this study had a large sample size of 374 participants ($N = 374$ in the online survey, $N = 12$ in the interviews) that should enable greater statistical power in the findings.

However, there are some study limitations that should also be noted. First, this study included self-report data. It is thus difficult to conclude whether certain findings are objectively true, such as whether SMEs have a capability in cyber security. This study identified that certain organizations (e.g. those in the Information Technology sector) implemented greater levels of cyber security than other sectors. It could be that such organizations may want to show themselves in a positive light given they are working in a field related to cyber security. This study is therefore relying on the opinions of participants in such areas, rather than an objective assessment. Second, although this study has made novel findings in our understanding of SMEs and cyber security, future similar research would benefit from furthering this knowledge by including a greater number of variables and more granularity within the variables. Third, while the survey included a substantial and diverse sample of SMEs, the results should be interpreted in light of certain boundaries of inference. The sample reflects organizations that were willing to participate in a study on cyber security and therefore may not capture the perspectives of SMEs that are less engaged with the topic. In addition, the design was cross sectional and conducted within the UK, which may influence how findings translate to different national or economic contexts. The analyses are therefore intended to identify patterns and relationships that are likely to be broadly relevant to SMEs, while recognizing that specific figures or magnitudes may vary across contexts. Fourth, although the interviews were conducted after the survey data collection, the survey data was not analyzed prior to the interviews taking place. One such advantage of this approach could have been to have asked specific questions within the interview process that directly related to findings identified in the survey analysis.

6. Conclusions

The current study examined how 1) cyber security controls, 2) awareness, knowledge, attitude, culture and 3) support routes vary across SME categories. Sole traders had the lowest amount of regular training and awareness programmes than organizations of other sizes. Industry leading organizations demonstrated higher engagement in the unadjusted analyses, while sector, particularly Information Technology, emerged as the most consistent independent predictor of implementation, awareness and support engagement in the multivariable models. Organizational size demonstrated selective but meaningful associations with controls and perceived capability, while sector consistently structured broader patterns of cyber security behavior. SMEs underestimate risks, with experience of having a cyber security attack influencing how they perceive risk. Some SMEs also take a biased view toward their own organization, specifically that they have a belief that their own employees have the skills and experience to handle cyber threats. SMEs are thus potentially overconfident in their view that their employees have the necessary skills and experience to handle cyber threats. Several SMEs reported limited awareness of available support routes, specifically they generally struggle to know where to go for support which may result in them defaulting to an I.T provider they have previously used. Resource constraints, particularly in the form of financial constraints, can also be a factor that hinders SMEs in adopting cyber security support. There are a number of implications from this study for policy and practice, not least for the NCSC in the UK to support organizations that are not categorized as Industry Leading or within Information Technology. The NCSC can outline the pressing need for these organizations to be doing more in relation to cyber security and also recommend how such organizations can improve their cyber security.

Author contributions

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

Disclosure statement

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

ORCID

Matthew Rand http://orcid.org/0009-0009-2446-0259
Maria Bada http://orcid.org/0000-0003-0741-5199
Steven Furnell http://orcid.org/0000-0003-0984-7542
Jason R.C. Nurse http://orcid.org/0000-0003-4118-1680
Neeshe Khan http://orcid.org/0000-0003-3962-7305

Funding

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

References

Adriko, R., & Nurse, J. R. C. (2024). Cybersecurity, cyber insurance and small-to-medium-sized enterprises: A systematic review. *Information and Computer Security*, *32*(5), 691–710. https://doi.org/10.1108/ICS-01-2024-0025

Adriko, R., & Nurse, J. R. C. (2026). Cybersecurity and cyber insurance for small to medium-sized enterprises (SMEs): Perceptions, challenges and decision-making dynamics. *Computers & Security*, *163*, 104818. https://doi.org/10.1016/j.cose.2025.104818

Ahmed, N. N., & Nanath, K. (2021). Exploring cybersecurity ecosystem in the Middle East: Towards an SME recommender system. *Journal of Cyber Security and Mobility*, *10*(3), 511–536. https://doi.org/10.13052/jcsm2245-1439.1032

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

Alshaikh, M., Maynard, S. B., & Ahmad, A. (2021). Applying social marketing to evaluate current security education training and awareness programs in organisations. *Computers & Security*, *100*, 102090. https://doi.org/10.1016/j.cose.2020.102090

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

Arroyabe, M. F., Arranz, C. F. A., Fernandez de Arroyabe, J. C., & Fernandez, I. (2024). Digitalization and cybersecurity in SMEs: A bibliometric analysis. *Procedia Computer Science*, *237*, 80–87. https://doi.org/10.1016/j.procs.2024.05.082

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information and Computer Security*, *27*(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? International Conference on Cyber Security for Sustainable Society (CSSS 2015) (pp. 118–131). Coventry, UK.

Barlette, Y., Gundolf, K., & Jaouen, A. (2017). Ceo´s information security behavior in SMEs: Does ownership matter? *Systemes D'Information Et Management*, *22*(3), 7–45. https://aisel.aisnet.org/sim/vol22/iss3/2

Barlette, Y., & Jaouen, A. (2019). Information security in SMEs: Determinants of CEOs' protective and supportive behaviors. *Systèmes D'Information Et Management*, *24*(3), 7–40. https://doi.org/10.3917/sim.193.0007

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing maturity models for IT management. *Business & Information Systems Engineering*, *1*(3), 213–222. https://doi.org/10.1007/s12599-009-0044-5

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Braun, V., & Clarke, V. (2021). *Thematic analysis: A practical guide*. Sage.

Carias, J. F., Borges, M. R. S., Labaka, L., Arrizabalaga, S., & Hernantes, J. (2020). Systematic approach to cyber resilience operationalization in SMEs. *IEEE Access*, *8*, 174200--174221. https://doi.org/10.1109/ACCESS.2020.3026063

Chaudhary, S., Gkioulos, V., & Goodman, D. (2023). Cybersecurity awareness for small and medium-sized enterprises (SMEs): Availability and scope of free and inexpensive awareness resources. In S. Katsikas (Ed.), *Computer security: ESORICS*, 2022 international workshops (LNCS 13785, pp. 97–115). Springer. https://doi.org/10.1007/978-3-031-25460-4_6

CMMI Product Team. (2018). CMMI for development (version 2.0). CMMI Institute. Retrieved February 18, 2026, from https://cmmiinstitute.com

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Lawrence Erlbaum Associates.

Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study. *Information and Computer Security*, *24* (2), 139–151. https://doi.org/10.1108/ICS-12-2015-0048

Davila, A., Foster, G., & Jia, N. (2010). Building sustainable high-growth startup companies: Management systems as an accelerator. *California Management Review*, *52*(3), 79–105. https://doi.org/10.1525/cmr.2010.52.3.79

De Haes, S., & Van Grembergen, W. (2009). An exploratory study into IT governance implementations and its impact on business/IT alignment. *Information Systems Management*, *26*(2), 123–137. https://doi.org/10.1080/10580530902794786

Department for Business and Trade. (2025, October 2). Business population estimates for the UK and regions 2025: Statistical release. GOV.UK. Retrieved February 13, 2026, from https://www.gov.uk/government/statistics/business-population-estimates-2025

DSIT. (2024, April 19). Cybersecurity breaches survey 2024. GOV.UK. Retrieved October 13, 2025, from https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024

DSIT. (2025, April 10). Cybersecurity breaches survey 2025. GOV.UK. Retrieved October 13, 2025, from https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025

ENISA. (2021). Enisa threat landscape 2021. Retrieved from. Retrieved October 13, 2025, from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Field, A. P. (2017). *Discovering statistics using IBM SPSS statistics* (5th ed.). Sage.

FSB. (2024). Uk small business statistics. Retrieved from. Retrieved October 13, 2025, from https://www.fsb.org.uk/media-centre/uk-small-business-statistics

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A cyber-security culture framework for assessing organization readiness. *Journal of Computer Information Systems*, *62*(3), 452–462. https://doi.org/10.1080/08874417.2020.1845583

Gerst, M., Kappe, M., Härting, R., & Karg, C. (2024). Determinants of the successful establishment of a cyber security culture in SMEs. *Procedia Computer Science*, *246*, 510–518. https://doi.org/10.1016/j.procs.2024.09.431

Goh, Z. J., & Singh, J. S. K. (2023). Digitalization and its impact on small and medium-sized enterprises (SMEs): An exploratory study of challenges and proposed solutions. *International Journal of Business and Technology Management*, *5*(4), 238–255. https://doi.org/10.55057/ijbtm.2023.5.4.22

Groß, T. (2021). Statistical reliability of 10 years of cyber security user studies. In T. Groß & L. Viganò (Eds.), *Stast 2020* (pp. 171–190). Springer. https://doi.org/10.1007/978-3-030-79318-0_10 (LNCS 12812.

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. *Field Methods*, *18*(1), 59–82. https://doi.org/10.1177/1525822X05279903

Gundu, T. (2019). Acknowledging and reducing the knowing and doing gap in employee cybersecurity compliance. ICCWS, 2019 14th International Conference on Cyber Warfare and Security (pp. 94–102). Stellenbosch, South Africa.

Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small businesses: An empirical examination. *Information Management & Computer Security*, *13*(4), 297–310. https://doi.org/10.1108/09685220510614425

Heidt, M., Gerlach, J. P., & Buxmann, P. (2019). Investigating the security divide between SME and large companies: How SME characteristics influence organisational IT security investments. *Information Systems Frontiers*, *21*(6), 1285–1305. https://doi.org/10.1007/s10796-019-09959-1

Hoppe, F., Gatzert, N., & Gruner, P. (2021). Cyber risk management in SMEs: Insights from industry surveys. *Journal of Risk Finance*, *22*(3/4), 240–260. https://doi.org/10.1108/JRF-02-2020-0024

Huaman, N., von Skarczinski, B., Stransky, C., Wermke, D., Acar, Y., Dreißigacker, A., & Fahl, S. (2021). A large-scale interview study on information security in and attacks against small and medium-sized enterprises. Proceedings of the 30th USENIX Security Symposium (USENIX Security 21) (pp. 1235–1252). USENIX Association. https://www.usenix.org/conference/usenixsecurity21/presentation/huaman

Ikuero, F. E., & Zeng, W. (2022). Improving cybersecurity incidents reporting in Nigeria: Micro and small enterprises perspectives. *Nigerian Journal of Technology*, *41*(3), 512–520. https://www.nijotech.com/index.php/nijotech/article/view/2958

Jafari-Sadeghi, V., Garcia-Perez, A., Candelo, E., & Couturier, J. (2021). Exploring the impact of digital transformation on technology entrepreneurship and technological market expansion: The role of technology readiness, exploration and exploitation. *The Journal of Business Research*, *124*, 100–111. https://doi.org/10.1016/j.jbusres.2020.11.020

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica*, *47*(2), 263–292. https://doi.org/10.2307/1914185

Kahneman, D., & Tversky, A. (1982). Intuitive prediction: Biases and corrective procedures. In D. Kahneman, P. Slovic, & A. Tversky (Eds.), *Judgment under uncertainty: Heuristics and biases* (pp. 414–421). Cambridge University Press. https://doi.org/10.1017/CBO9780511809477.031

Kaila, U., & Nyman, L. (2018). Information security best practices: First steps for startups and SMEs. *Technology Innovation Management Review*, *8*(11), 32–42. https://doi.org/10.22215/timreview/1198

Kaur, J., & Mustafa, N. A. (2013). Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME. 2013 International Conference on Research and Innovation in Information Systems (ICRIIS) (pp. 286–290). Kuala Lumpur, Malaysia. https://doi.org/10.1109/ICRIIS.2013.6716723

Kesswani, N., & Kumar, S. (2015). Maintaining cyber security: Implications, cost and returns. Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research (pp. 161–164). Association for Computer Machinery, New York. https://doi.org/10.1145/2751957.2751976

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. https://doi.org/10.1016/j.cose.2025.104448

Ključnikov, A., Mura, L., & Sklenár, D. (2019). Information security management in SMEs: Factors of success. *Entrepreneurship & Sustainability Issues*, *6*(4), 2081–2094. https://doi.org/10.9770/jesi.2019.6.4(37)

Lee, Y., & Larsen, K. (2009). Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(2), 177–187. https://doi.org/10.1057/ejis.2009.11

Levie, J., & Lichtenstein, B. B. (2010). A terminal assessment of stages theory: Introducing a dynamic states approach to entrepreneurship. *Entrepreneurship Theory and Practice*, *34*(2), 317–350. https://doi.org/10.1111/j.1540-6520.2010.00377.x

Li, L., Xu, L., & He, W. (2022). The effects of antecedents and mediating factors on cybersecurity protection behavior. *Computers in Human Behavior Reports*, *5*, 100165. https://doi.org/10.1016/j.chbr.2021.100165

Manzoor, J., Waleed, A., Jamali, A. F., & Masood, A. (2024). Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs. *PLOS*

ONE, *19*(3), e0301183. https://doi.org/10.1371/journal.pone.0301183

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, *69*(1), 151–156. https://doi.org/10.1016/j.chb.2016.11.065

Metin, B., Özhan, F. G., & Wynn, M. (2024). Digitalisation and cybersecurity: Towards an operational framework. *Electronics*, *13*(21), 4226. https://doi.org/10.3390/electronics13214226

Michie, S., Atkins, L., & West, R. (2014). *The behaviour change wheel book: A guide to designing interventions*. Silverback.

Mitrofan, A.-L., Cruceru, E.-V., & Barbu, A. (2020). Determining the main causes that lead to cybersecurity risks in SMEs. *Business Excellence and Management*, *10* (4), 38–48. https://doi.org/10.24818/beman/2020.10.4-03

NCSC. (2020). Small business guide: Cyber security. Retrieved October 13, 2025, from https://www.ncsc.gov.uk/collection/small-business-guide

Norman, G. (2010). Likert scales, levels of measurement and the "laws" of statistics. *Advances in Health Sciences Education*, *15*(5), 625–632. https://doi.org/10.1007/s10459-010-9222-y

Obreja, D., Rughiniș, R., & Țurcanu, D. (2025). What drives new knowledge in human cybersecurity behavior? Insights from bibliometrics and thematic review. *Computers in Human Behavior Reports*, *18*, 100650. https://doi.org/10.1016/j.chbr.2025.100650

OECD. (2023). Oecd sme and entrepreneurship outlook 2023. Retrieved October 13, 2025, from https://www.oecd.org/en/publications/2023/06/oecd-sme-and-entrepreneurship-outlook-2023_c5ac21d0.html

Office for National Statistics. (2024, September 25). Uk business; activity, size and location: 2024. Retrieved February 13, 2026, from https://www.ons.gov.uk/businessindustryandtrade/business/activitysizeandlocation/bulletins/ukbusinessactivitysizeandlocation/2024?

Osborn, E., & Simpson, A. (2018). Risk and the small-scale cyber security decision making dialogue-a UK case study. *The Computer Journal*, *61*(4), 472–495. https://doi.org/10.1093/comjnl/bxx093

Osborn, E., & Simpson, A. C. (2017). On small-scale it users' system architectures and cyber security: A UK case study. *Computers & Security*, *70*, 27–50. https://doi.org/10.1016/j.cose.2017.05.001

Paulk, M. C., Curtis, B., Chrissis, M. B., & Weber, C. V. (1993). Capability maturity model, version 1.1. *IEEE Software*, *10*(4), 18–27. https://doi.org/10.1109/52.219617

Pawar, S. A., & Palivela, H. (2023). Importance of least cybersecurity controls for small and medium enterprises (SMEs) for better global digitalised economy. In P. Tyagi, S. Grima, K. Sood, B. Balamurugan, E. Özen, & E. Thalassinos (Eds.), *Smart analytics, artificial intelligence and sustainable performance management in a global digitalised economy* (Vol. 110, pp. 21–53). Emerald Publishing Limited. https://doi.org/10.1108/S1569-37592023000110B002.

Pawar, S., & Palivela, H. (2022). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). *International Journal of Information Management Data Insights*, *2*(1), 100080. https://doi.org/10.1016/j.jjimei.2022.100080

Phelps, R., Adams, R., & Bessant, J. (2007). Life cycles of growing organizations: A review with implications for knowledge and learning. *International Journal of Management Reviews*, *9*(1), 1–30. https://doi.org/10.1111/j.1468-2370.2007.00200.x

Rabii, A., Assoul, S., Ouazzani Touhami, K., & Roudies, O. (2020). Information and cyber security maturity models: A systematic literature review. *Information and Computer Security*, *28*(4), 627–644. https://doi.org/10.1108/ICS-03-2019-0039

Rae, A., & Patel, A. (2019). Defining a new composite cybersecurity rating scheme for SMEs in the U.K. In S.-H. Heng & J. Lopez (Eds.. Information Security Practice and Experience: 15th International Conference, ISPEC 2019, Kuala Lumpur, Malaysia, November 26-28, 2019, Proceedings (Lecture Notes in Computer Science (Vol. 11879. pp. 362–380). Springer. https://doi.org/10.1007/978-3-030-34339-2_20

Rae, A., & Patel, A. (2020). Developing a security behavioural assessment approach for cyber rating UK MSBs. Proceedings of the 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security) (pp. 1–8). Dublin, Ireland: IEEE. https://doi.org/10.1109/CyberSecurity49315.2020.9138893

Renaud, K., & Ophoff, J. (2021). What is preventing UK SMEs from taking cyber security precautions? Retrieved October 13, 2025, from https://www.muster.scot/docs/MUSTER_White_Paper.pdf

Renaud, K., & Weir, G. (2016). Cybersecurity and the unbearability of uncertainty. 2016 Cybersecurity and Cyberforensics Conference (CCC) (pp. 137–143). Amman, Jordan: IEEE. https://doi.org/10.1109/CCC.2016.29

Ryan, R. M., & Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *The American Psychologist*, *55*(1), 68–78. https://doi.org/10.1037/0003-066X.55.1.68

Saban, K. A., Rau, S., & Wood, C. A. (2021). Sme executives' perceptions and the information security preparedness model. *Information and Computer Security*, *29*(2), 263–282. https://doi.org/10.1108/ICS-01-2020-0014

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for business resilience: Issues and recommendations. *Sensors*, *23*(15), 6666. https://doi.org/10.3390/s23156666

Santos-Olmo, A., Sánchez, L. E., Caballero, I., Camacho, S., & Fernandez-Medina, E. (2016). The importance of the security culture in SMEs as regards the correct management of the security of their assets. *Future Internet*, *8*(3), 30. https://doi.org/10.3390/fi8030030

Shojaifar, A., & Järvinen, H. (2021). Classifying SMEs for approaching cybersecurity competence and awareness. The 16th International Conference on Availability, Reliability and Security (pp. 1–7). Vienna, Austria. https://doi.org/10.1145/3465481.3469200

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Stewart, G., & Lacey, D. (2012). Death by a thousand facts: Criticising the technocratic approach to information security awareness. *Information Management & Computer Security*, *20*(1), 29–38. https://doi.org/10.1108/09685221211219182

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, *109*, 102387. https://doi.org/10.1016/j.cose.2021.102387

Ulrich, P., Frank, V., & Timmermann, A. (2020). The dark side of data science - an empirical study of cyber risks in German SMEs. *Procedia Computer Science*, *176*, 2615–2624. https://doi.org/10.1016/j.procs.2020.09.307

Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, *75*(1), 547–559. https://doi.org/10.1016/j.chb.2017.05.038

Verizon. (2023). 2023 Data Breach Investigations Report. Retrieved from Available from: Retrieved October 13, 2025, from https://www.verizon.com/business/resources/Tce6/reports/2023-dbir-smb-snapshot.pdf

Verizon. (2024). 2024 Data Breach Investigations Report. Retrieved from. Retrieved October 13, 2025, from https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

Wilson, M., McDonald, S., Button, D., & McGarry, K. (2023). It won't happen to me: Surveying SME attitudes to cyber-security. *Journal of Computer Information Systems*, *63*(2), 397–409. https://doi.org/10.1080/08874417.2022.2067791

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

Yigit Ozkan, B., & Spruit, M. (2022). Adaptable security maturity assessment and standardization for digital SMEs. *Journal of Computer Information Systems*, *63*(4), 965–987. https://doi.org/10.1080/08874417.2022.2119442

Zhou, Q., Li, B., Scheibenzuber, C., & Li, H. (2023). Fake news land? Exploring the impact of social media affordances on user behavioral responses: A mixed-methods research. *Computers in Human Behavior*, *148*, 107889. https://doi.org/10.1016/j.chb.2023.107889