Cybersecurity Awareness and Capacities of SMEs

Gencer Erdogan[1][a], Ragnhild Halvorsrud[1][b], Costas Boletsis[1][c], Simeon Tverdal[1][d]
and John Brian Pickering[2][e]

[1] *Sustainable Communication Technologies, SINTEF Digital, Oslo, Norway*

[2] *IT Innovation Centre, University of Southampton, Southampton, U.K.*

Keywords: Cybersecurity, Cyber Risk, Awareness, Capacity, Practice, SME, Survey.

Abstract: Small and Medium Enterprises (SMEs) are increasingly exposed to cyber risks. Some of the main reasons include budget constraints, the employees' lack of cybersecurity awareness, cross-sectoral cyber risks, lack of security practices at organizational level, and so on. To equip SMEs with appropriate tools and guidelines that help mitigate their exposure to cyber risk, we must better understand the SMEs' context and their needs. Thus, the contribution of this paper is a survey based on responses collected from 141 SMEs based in the UK, where the objective is to obtain information to better understand their level of cybersecurity awareness and practices they apply to protect against cyber risks. Our results indicate that although SMEs do apply some basic cybersecurity measures to mitigate cyber risks, there is a general lack of cybersecurity awareness and lack of processes and tools to improve cybersecurity practices. Our findings provide to the cybersecurity community a better understanding of the SME context in terms of cybersecurity awareness and cybersecurity practices, and may be used as a foundation to further develop appropriate tools and processes to strengthen the cybersecurity of SMEs.

1 INTRODUCTION

Small and Medium Enterprises (SMEs) are increasingly exposed to cyber risks. According to Khan et al., 61% of SMEs were exposed in 2017 to malware cyberattacks (Khan et al., 2020). Recent reports from across the industry paint a disturbing picture about overall vulnerabilities. According to a Ponemon Institute report, 67% of SMEs experienced a cyberattack and 58% experienced data breach in 2018, while Beazley Group report that 71% of ransomware attacks are aimed at SMEs (Roy, Mekhala, 2021). The European Union Agency for Cybersecurity (ENISA) reports on real life incidents SMEs are frequently exposed to, including ransomware, hijacking email accounts, and phishing (ENISA, 2021). Among eight cybersecurity challenges for SMEs identified by ENISA, low cybersecurity awareness is ranked as number one.

Despite the increasing exposure to cyber risks, SMEs often underestimate this threat and invest less in cybersecurity measures due to budget constraints (Saleem et al., 2017). However, the lack of investment in security is not solely related to budget constraints. Individual employees represent a significant vulnerability (Vakakis et al., 2019). Further, since SMEs typically operate as co-competitors within a single supply-chain alongside other SMEs, risk may propagate to others (Lewis et al., 2014). At the same time, there is a generalised lack of cybersecurity information specialized for SMEs to help them address cyber risks (Gafni and Pavel, 2019; ENISA, 2021). Moreover, organizational IT security research has largely neglected the SME context, which negatively influences the SMEs' cybersecurity investments (Heidt et al., 2019). Thus, to understand the needs of SMEs in terms of cybersecurity knowledge, and what guidelines and tools may be required, we need to investigate the cybersecurity awareness and cybersecurity practices conducted in SMEs.

The contribution of this paper is a survey based on responses collected from 141 SMEs based in the UK. We employ survey research to collect and analyze data from the SMEs, and the objective of our study is to obtain information about their level of cybersecurity awareness and cybersecurity practices based on

[a] https://orcid.org/0000-0001-9407-5748
[b] https://orcid.org/0000-0002-3774-4287
[c] https://orcid.org/0000-0003-2741-8127
[d] https://orcid.org/0000-0003-1660-4127
[e] https://orcid.org/0000-0002-6815-2938

Erdogan, G., Halvorsrud, R., Boletsis, C., Tverdal, S. and Pickering, J.
Cybersecurity Awareness and Capacities of SMEs.
DOI: 10.5220/0011609600003405
In *Proceedings of the 9th International Conference on Information Systems Security and Privacy (ICISSP 2023)*, pages 296-304
ISBN: 978-989-758-624-8; ISSN: 2184-4356

their answers to the questions in the survey. Thus, our overall research question is: *what is the level of cybersecurity awareness and cybersecurity practices of SMEs based in the UK?*

The survey consisted of 27 questions: 5 questions about the company in general, 4 questions about the participant, 4 questions about the company infrastructure, 8 questions related to cybersecurity awareness, 5 questions related to cybersecurity practices, and finally one question to collect general feedback about the survey. In this paper, we focus mainly on the questions and answers related to cybersecurity awareness and cybersecurity practices. However, we have made the complete data set of questions and answers from the 141 SMEs available online [1] to show transparency to our study and provide the data for further research.

Our results indicate that although SMEs do apply some basic cybersecurity measures to mitigate cyber risks, there is a general lack of cybersecurity awareness and lack of processes and tools to improve cybersecurity practices.

The remainder of this paper is organized as follows. Section 2 describes the design and execution of the survey, while Section 3 describes the results obtained. In Section 4, we discuss the results with respect to cybersecurity awareness and cybersecurity practices of the SMEs. Section 5 describes limitations of our work, while Section 6 relates our work to similar surveys. Finally, we provide concluding remarks in Section 7.

2 SURVEY

An online survey was designed to capture the cybersecurity practices in SMEs. Since information about cybersecurity practices is potentially very sensitive and business-critical, an anonymous survey was developed.

2.1 Target Group

The target group of the survey were the SMEs' employees, and we recruited one employee from each of the 141 SMEs included in the survey. To define the recruitment field, i.e., SMEs, we used the European Commission's definition of SME based on the staff headcount (European Commission, 2016), i.e., enterprises that employ fewer than 250 persons.

Three main subgroups were identified as sources for establishing the needed knowledge: 1) persons/roles responsible for cybersecurity, 2) management, and 3) other employees, in general.

2.2 Sampling and Data Collection

Participants were recruited through the Norstat recruitment agency for online research[2]. A recruitment agency was used due to the specialised and private nature of the examined topic. For this study, UK was chosen as the country to recruit participants from because of i) practical considerations, i.e., approaching respondents in their native language and ii) the importance of cybersecurity awareness for UK companies since four in ten UK-based businesses (39%) report having cybersecurity breaches or attacks during the last 12 months, based on the 2021 UK Government's cybersecurity breaches survey (DCMS, Ipsos MORI, 2021). The participation of the survey was anonymous and in compliance with ethical requirements for involvement of humans in research, including voluntariness and informed consent.

The online survey was implemented using the QuenchTec[3] survey platform, which includes modules for survey design and data collection. The survey was launched in October 2020 and ran for two weeks.

2.3 Questionnaire Design

The questionnaire was developed iteratively and piloted with $N = 23$ participants, who were recruited using proximity sampling. As a result, the questions were shaped according to the received feedback from the 23 participants. This iterative development of the questions was conducted to make sure that our questions capture the necessary information to answer our overall research question. The completion time for the final survey was estimated to 10–15 minutes.

The final survey consisted of 27 questions in total. The questions were a mix of closed multiple-response items (tick boxes) or single-response items (radio buttons), often in combination with text input fields for open-ended questions, e.g., "Please provide further information". The questions were organised into five thematic sections:

1. Information about the company: business sector, size, and main operation. This section had five questions in total.
2. Information about the participant: job title, role(s), responsibilities, and years of employment. This section had four questions in total.

[1] https://doi.org/10.5281/zenodo.7443048

[2] https://norstatgroup.com/

[3] https://quenchtec.com

3. Information about the company infrastructure: the usage of technology in the company, outsourcing, usage of cloud services, customers or partners that share the company infrastructure. This section had four questions in total.
4. Information about cybersecurity awareness: the company's work in raising awareness about cybersecurity for employees, positions dedicated to cybersecurity, whether cybersecurity is raised as an agenda item in meetings and in general, how employees characterize their own cybersecurity knowledge, the company's awareness about cybersecurity, the fear of cybersecurity attacks, whether the company has been exposed to cyber attacks previously, and if yes, characterization of their impact. This section had eight questions in total.
5. Information about cybersecurity practices: the company's threshold to downtime of critical applications and systems, measures taken to avoid cybersecurity attacks, specific processes or tools to assess cyber-risks, identify vulnerabilities, and identify cyber attacks. This section had five questions in total.

In addition to the number of questions in the sections described above, there was a final question to collect general feedback about the survey. Thus, there was a total of 27 questions.

2.3.1 Selected Questions

In the rest of the paper, we will focus on the results of the 13 questions related specifically to cybersecurity awareness (Point 4 in Section 2.3) and cybersecurity practices (Point 5 in Section 2.3). Before we provide the results in Section 3 and discuss the results in Section 4, the questions are presented, as follows:

Questions related to cybersecurity awareness (eight questions):

Q1 Does your company offer courses or training material for employees to raise awareness about cybersecurity?

Q2 Does your company have positions dedicated to cybersecurity at any level?

Q3 Do you discuss cybersecurity issues on your company meetings or presentations or, in general, internally in your company?

Q4 How would you characterize your own knowledge about cybersecurity?

Q5 To what degree do you fear for a cybersecurity attack towards your company?

Q6 How would you characterize your company when it comes to cybersecurity awareness?

Q7 Were there any previous cybersecurity attacks on your company that you know about?

Q8 What was the impact of the cybersecurity attack(s)? (only if ”yes” to Q7)

Questions related to cybersecurity practices (five questions):

Q9 How long do you think your critical applications and systems can be shut down before significant disruption is caused to the company?

Q10 What security measures is your company taking to avoid cybersecurity attacks?

Q11 Does your company use specific processes or tools to assess risk to its IT assets?

Q12 Does your company use specific processes or tools for identifying cybersecurity vulnerabilities?

Q13 Does your company use specific processes or tools for identifying cybersecurity attacks?

3 RESULTS

The online survey collected 150 responses and results were analysed using IBM SPSS and Microsoft Excel. Nine (9) respondents were excluded: six of them (6) were pensioners, one (1) was a freelancer, and two (2) were unemployed. Their participation did not therefore conform with the inclusion criterion of working at an SME. After filtering the final sample size was $N = 141$.

The following presents the results from the selected questions (Section 2.3.1), i.e., the questions related to cybersecurity awareness (Q1–Q8) and cybersecurity practices (Q9–Q13).

3.1 Cybersecurity Awareness

The participants representing the SMEs characterized their own knowledge about cybersecurity (Q4) as follows: 19 out of 141 (13%) answered *expert*, 52 (37%) answered *moderate knowledge*, 57 (40%) answered *basic knowledge*, and 13 (9%) answered *no knowledge* (see Figure 1). That is, only half of the respondents ($19 + 52 = 71$ or 50.4%) characterize their own knowledge about cybersecurity as moderate or expert.

The participants were also asked to characterize their company's level of cybersecurity awareness (Q6): 37 out of 141 (26%) answered *high awareness*, 76 (54%) answered *moderate awareness*, 22 (16%)

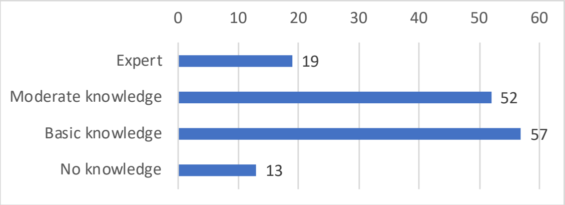

Figure 1: The participants' knowledge about cybersecurity (Q4).

answered *low awareness*, and 6 (4%) answered *I do not know* (see Figure 2). That is, 113 out of 141 SMEs (80%) answered that their company has moderate to high awareness of cybersecurity.

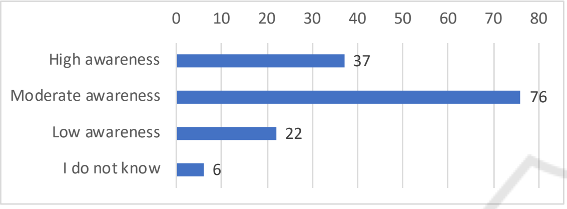

Figure 2: The companies' level of cybersecurity awareness (Q6).

With respect to offering courses or training material for employees to raise awareness of cybersecurity (Q1), and despite the moderate to high awareness of risk (Q6), only 27 out of 141 (19%) confirm that they do provide cybersecurity training for their employees, while 103 (73%) replied that they do not provide such training, and 11 (8%) were not sure (see Figure 6). Moreover, the 27 SMEs that do offer training for employees provided additional information indicating the kind of topics covered by their courses/training capacities. The topics addressed are mainly basics related to security and privacy the employees need to be aware of when using computers on-site at work with which the training is provided is typically when an employee joins the company, and at the best case, some companies have yearly repetitions of the courses/training. This seems inconsistent with the earlier claim that awareness is high or moderate (ca. 50% for Q4). Figure 3 shows the distribution of the 27 SMEs with respect to the industry sector they operate in. We see that 6 operate in legal and professional services, 6 in industrial/manufacturing/construction, 5 in financial services, 3 in retail, and 7 in the *other* category, where each of the seven companies represent one of the following industry sectors: public sector, leisure and travel, education and research, communication and mobile, childcare, engineering, health and pharmaceuticals. Industry coverage is therefore good.

When asked whether the SME has any positions dedicated to cybersecurity (Q2), 45 out of 141 (32%) answered *yes*, 85 (60%) answered *no*, and 11 (8%) answered *I do not know*. That is, about 1/3 confirm that their SME have positions dedicated to cybersecurity (see Figure 6). Having cybersecurity on the agenda in daily operation will inevitably make employees more aware of cybersecurity. So the participants were asked whether they discuss cybersecurity issues in meetings, presentations, or in general internally in the company (Q3). This question revealed that about 1/3 never discuss cybersecurity (see Figure 4). That is, 20 out of 141 (14%) answered that they discuss cybersecurity issues *all the time*, 70 (50%) answered *sometimes*, and 51 (36%) answered *not at all*.

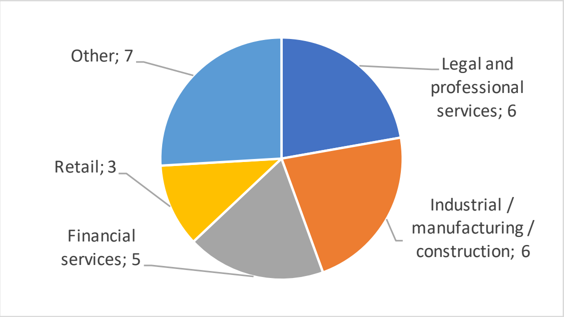

Figure 3: SMEs offering cybersecurity training, grouped by industry sector.

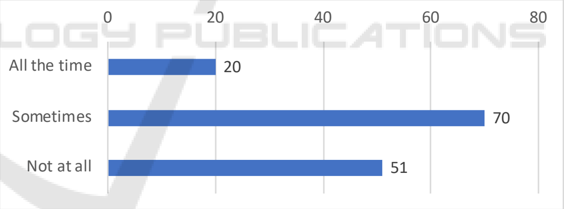

Figure 4: Discussing cybersecurity issues in the company (Q3).

To obtain an overall understanding of the SMEs' concerns about cybersecurity, they were also asked the degree to which they feared a cybersecurity attack on their company (Q5). The answers show that 11 out of 141 (8%) fear cybersecurity attacks *a lot*, 74 (52%) answered *moderately*, while 56 (40%) answered *not at all* (see Figure 5).

Moreover, the participants were asked whether they were aware of any previous cybersecurity attacks on their companies (Q7). As illustrated in Figure 6, 21 out of 141 (15%) answered *yes*, 109 (77%) answered *no*, and 11 (8%) answered *I do not know*. A cybersecurity attack may cause harm to one or more security qualities represented by the CIA-triad (Confidentiality, Integrity, and Availability). The 21 participants

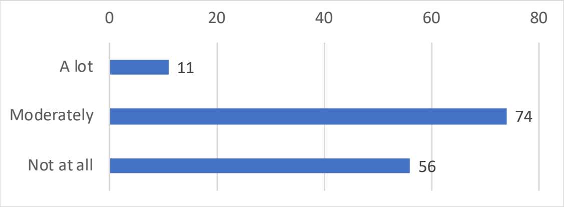

Figure 5: Fear of cybersecurity attack on the company (Q5).

who answered *yes* were then asked about the impact that those attacks caused (Q8), therefore. Responses revealed that 12 of the attacks altered the integrity of information, 11 attacks rendered the information systems unavailable, while 6 of the attacks caused a breach of confidential information.

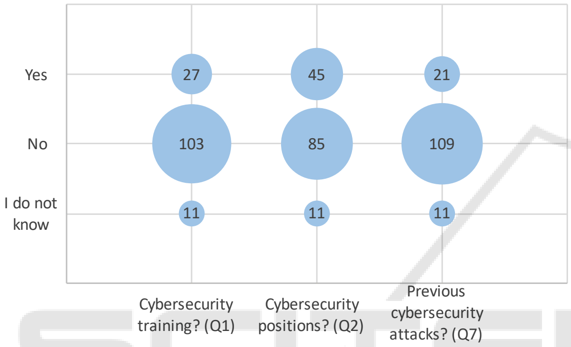

Figure 6: Answers to Q1, Q2, Q7.

3.2 Cybersecurity Practices

Concerning security measures to avoid cybersecurity attacks (Q10), the participants were presented with a list of measures from which they could select one or more of the options that applied for their company. The list of security measures and the number of ticks each option received are shown in Figure 7[4]. We see that five of the security measures distinguish themselves in popularity. The most common defences were anti-virus software (selected by 93 out of 141), firewalls to prevent remote access to internal networks (selected by 88 out of 141), access control to prevent unauthorized access to data and services (selected by 84 out of 141), software updates to remove existing vulnerabilities (selected by 80 out of 141), and ensuring appropriate configuration for security on all devices and software (selected by 78 out of 141).

The security measures that are less used include stronger forms of authentication such as 2-factor authentication or public key certification (selected by 41 out of 141), staff security training (selected by 38 out of 141), encrypted storage of data (selected by 33 out of 141), encrypted communications (selected by 27 out of 141), intrusion detection (selected by 27 out of 141), and bandwidth management on key network connections (selected by 14 out of 141). In addition, 16 participants did not know what kind of security measures were used in their company, while one participant replied that they have no online presence.

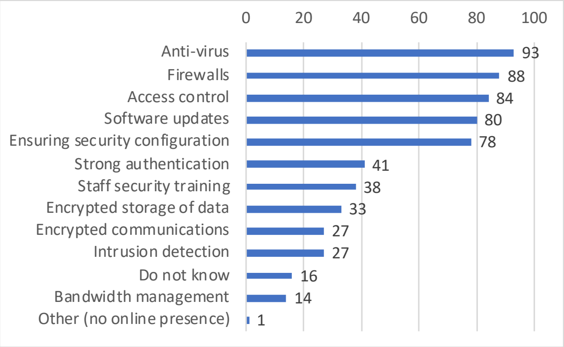

Figure 7: Security measures to avoid cybersecurity attacks (Q10).

Some variants of security attacks, such as Distributed Denial of Service (DDoS) attacks, aim to make the victim's target systems unavailable. Such attacks may cause significant disruption to businesses. When asked how long the participants thought their critical applications and systems can be shut down before significant disruption is caused to the company (Q9), 12 out of 141 (9%) replied *0 - 1 hour*, 24 (17%) replied *1 - 6 hours*, 33 (24%) replied *6 hours - 1 day*, 41 (29%) replied *more than 1 day*, and 31 (22%) replied *I do not know* (see Figure 8).

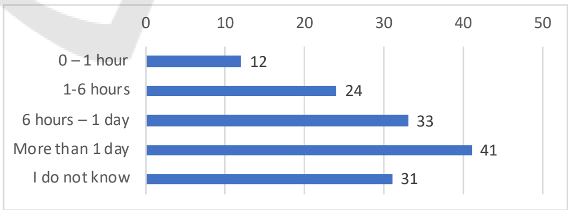

Figure 8: The time critical applications can be shut down before significant disruption to business (Q9).

The survey also included three questions asking whether the SMEs use any processes or tools to assess cybersecurity risks to its IT assets (Q11), identify cybersecurity vulnerabilities (Q12), and identify cybersecurity attacks (Q13). The replies to these questions are illustrated in Figure 9.

Regarding the question to whether the SME uses any tools to assess risks to its IT assets, 18 out of 141 (13%) answered *yes*, 92 out of 141 (65%) answered *no*, and 31 out of 141 (22%) answered *I do not know*.

[4] Note: a single SME may identify more than one measure.

Risk assessment is therefore not widely implemented in SMEs.

When asked whether the SME uses any tools to identify cybersecurity vulnerabilities, 22 (16%) answered *yes*, 87 (62%) answered *no*, and 32 (23%) answered *I do not know*. As with risk assessment, there is therefore little awareness of vulnerabilities.

Finally, regarding the question to whether the SME uses any tools to identify cybersecurity attacks, 19 (13%) answered *yes*, 87 (62%) answered *no*, and 35 (25%) answered *I do not know*. It follows, therefore, that attacks may go unreported or simply unnoticed.

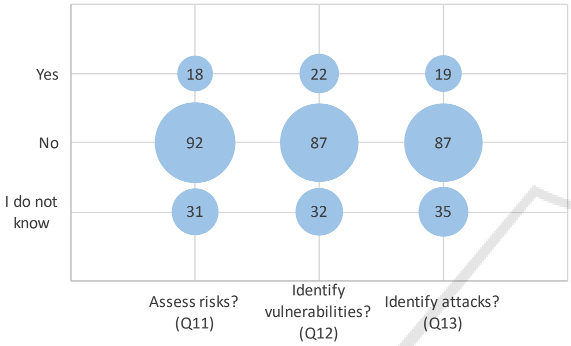

Figure 9: Answers to Q11, Q12, Q13.

4 DISCUSSION

In the following, we discuss our general observations about the results in Section 3, as well as our specific observations related to cybersecurity awareness and cybersecurity practices.

4.1 General Observations

The results of this survey highlight a number of general themes: a lack of awareness about preventative measures around cybersecurity (that is approximately 20% of ”Don’t know” type answers to Q11, Q12, and Q13; see Figure 9), and an apparent discrepancy between the levels of awareness and knowledge claimed by individuals (71 claiming moderate to expert knowledge Q4 from Figure 1) and companies (113 claiming moderate to high awareness in Q6 from Figure 2) by contrast to their willingness to take appropriate steps to mitigate risks. Apart from the potential impact on the SMEs themselves (36 out of 141 outages of less than 6 hours; and 31 ”Don’t know” in Figure 8), this is a concern for SME partners (Lewis et al., 2014): failing to take steps to mitigate risks is not only an issue for individual SMEs, but could also affect other businesses. Looking at individual and company responses, it is well-attested that what people say they will do (for instance, respond to cyber risks) and what they actually do may differ (Sheeran and Webb, 2016). By way of explanation, we know that information overload (Smerecnik et al., 2012) can prevent action. The SMEs may be aware, as they report, but are overwhelmed by the extent of the problem. This is consistent with the level of concern expressed ($11+74=85$ or 60% responding ’moderate’ or ’a lot’ of concern about possible attacks to Q5 in Figure 5). More specifically, though, the lack of focus (121 or 86% reporting discussion of cybersecurity as ”Not at all” or only ”Sometimes” in Q3; see Figure 4) and training (Q1), dedicated positions (Q2), awareness of attacks (Q7) (see Figure 6) suggests a level of unresponsiveness which may reflect that SMEs do not feel responsible to take action (Bada et al., 2019). With these points in mind, we consider specifically *Cybersecurity Awareness* and *Cybersecurity Practices* in the following sections.

4.2 Cybersecurity Awareness

When comparing the answers for Q4 and Q6, an interesting observation is that half (71 out of 114) of the participants characterize their own knowledge about cybersecurity as moderate or expert. Looking closer at the answers provided, we see that only 51 out of the 71 are in fact working with cybersecurity. Moreover, 113 out of 114 participants indicate that their company have moderate or higher awareness of cybersecurity. It is therefore reasonable to argue that the SMEs perception about their own cybersecurity awareness is rather more optimistic than it should be, compared to recent cybersecurity risk reports showing that SMEs are one of the most exposed group to cybersecurity attacks and vulnerabilities (Hoppe et al., 2021; Pugnetti and Casián, 2021). Secondly, participants are rather cautious about claiming that they have strong awareness of cybersecurity awareness, compared to when assessing the level of their SMEs awareness (which is assessed to be of higher awareness in cybersecurity). This could be an indication that people tend to trust that cybersecurity is dealt with in other parts of the company or by other people (such as third party services they may use as part of their business infrastructure). In the context of the general observations above, individuals within SMEs don’t only need the awareness, but must also accept their responsibility in maintaining robust defences against cyber risks (Paek and Hove, 2017).

Cybersecurity training facilities like cyber ranges are increasingly being used to develop cybersecurity skills (Yamin et al., 2020). Such facilities are important to help SMEs in building a strong security culture and maintain robust defences against cyber risks. However, these training facilities typically focus mainly on hands-on exercises and not learning and educational aspects (Erdogan et al., 2021; Erdogan et al., 2020). It is encouraging to see that a variety of SMEs are adopting some form of cybersecurity training (see Figure 3). However, the fact that only 27 out of 141 SMEs in our survey are providing cybersecurity training (at a very basic level) is a strong indication for the need of more easily available and pedagogical tools and guidelines to support SMEs for an easy uptake to increase their cybersecurity awareness.

In order to successfully raise awareness of cybersecurity and support employees in cybersecurity training, the SMEs need personnel who are knowledgeable in the domain of cybersecurity training and who have the skills to train other people. Our survey shows that only 45 out of 141 SMEs have positions dedicated to cybersecurity and that only 27 out of 141 SMEs provide cybersecurity training. Thus, 18 out of 141 SMEs that have positions dedicated to cybersecurity do not offer cybersecurity training. There can of course be many reasons to why these 18 SMEs do not offer cybersecurity training, but we believe that one important lesson here is that appropriate training must also be given to cybersecurity experts so that they are equipped with the tools necessary to provide cybersecurity training of people who are not experts in the domain.

4.3 Cybersecurity Practices

With respect to cybersecurity practices, one obvious observation is that barely any of the SMEs use tools or have processes in place to assess cybersecurity risks they are exposed to (Q11), identify potential vulnerabilities that may be exploited by an adversary (Q12), and identify cybersecurity attacks (Q13) (see Figure 9). This is entirely consistent with the observations in the previous two sections. But it may also indicate a lack of appropriate tooling to encourage awareness, and more importantly, to present appropriate and adaptive behaviours easy - such as implementing cybersecurity measures: responses to Q10 indicate that some are already in place (Figure 7). The issue now is not just to train individual employees and increase the understanding of personal risk (Von Solms and Van Niekerk, 2013) - making the risk personally relevant - but also their self-efficacy (Raineri and Resig, 2020) - making the risk individually manageable.

5 LIMITATIONS

It is easy to criticise quantitative studies for the number of responses obtained and the generalisability of the cohort of respondents. We believe, however, that there is enough consistency in the responses we have reported here to identify some general trends which are worthy of further investigation.

We also maintain that the assertions in the survey itself, validated by domain experts, provide coverage of the issues which SMEs currently face. Further, that the industry coverage reported indicates that the responses we have obtained across those industries suggest that the conclusions are relevant to SMEs in general.

Finally, relating our findings to what is known from the literature also suggests that the survey has highlighted appropriate areas of concern which can be taken forward in future work.

6 RELATED WORK

An online survey conducted by Wilson et al. (Wilson et al., 2022) surveys 85 U.K-based SMEs. While their survey focuses mainly on the SMEs' attitudes toward cybersecurity, our survey focuses on the cybersecurity awareness and practices of 141 U.K-based SMEs. Further, Wilson et al. (Wilson et al., 2022) suggest that while some SMEs are able to carry out preventative measures to avoid phishing attacks and strengthen mobile security, generally they still discount the risk of cyber attacks. This is also in line with our study in the sense that cybersecurity practices of SMEs are at a basic level in terms of using anti-virus, firewalls, access control, etc. Additionally, Wilson et al. focus on just three constructs from Protection Motivation Theory and find only partial support for their research hypotheses (Wilson et al., 2022). In particular, they find evidence of self-efficacy, in relation to some but not all common attack types. This is consistent with the literature on cybersecurity attitudes: individual employees feel it is not their responsibility to respond (Paek and Hove, 2017), or they're overwhelmed (Witte and Allen, 2000) (i.e., non-existent self-efficacy). Our study, therefore, provides more in-depth information about the cybersecurity and awareness context within SMEs to refine the type of education and training Wilson et al. recommend (Wilson et al., 2022). Further, respondents to their survey report that management need to take more action (i.e., responsibility is not theirs individually). Conversely, managers report having to focus on their core business rather than cybersecurity. Our survey provides a clearer picture of what they claim and what actually happens. For instance, although Wilson et al. (Wilson et al., 2022) call for specific, prerecorded training, we found that such training tended to be confined to on-boarding. Our survey therefore complements their findings within the broader context of individual employee response to cyber risks.

Ncubukezi et al. (Ncubukezi et al., 2020) carried out a survey on 30 South African SMEs where the objective was to investigate the cyber hygiene of the companies. Cyber hygiene is basically the overall practice to maintain good cybersecurity and safety (Ncubukezi et al., 2020). The study by Ncubukezi et al. concludes that SMEs are struggling to maintain good cybersecurity practices, and that companies pay little attention to balanced cybersecurity. With respect to cybersecurity practices, our survey reveals similar results and in addition includes the aspect of cybersecurity awareness which is not covered in the aforementioned study.

Senarathna et al. (Senarathna et al., 2016) carried out a survey on 150 Australian SMEs where they examined the influence of privacy and security factors on cloud adoption. Their findings show that security and privacy factors are not significantly influential for Australian SMEs when deciding whether to adopt cloud solutions. Although the survey by Senarathna et al. (Senarathna et al., 2016) did not intend to address cybersecurity awareness or cybersecurity practices like in our study, their findings do indicate that the SMEs may not have been fully aware of potential security and privacy risks as part of the decision making process for cloud adoption, which in turn raises the obvious need for increasing cybersecurity awareness.

Heidt et al. (Heidt et al., 2019) carried out a literature review, as well as 25 interviews with domain experts, to investigate how SME characteristics influence organizational IT security investments. Their study shows that the security literature typically does some wrong assumptions in the context of SMEs related to, for example, the presence of skilled workforce, documented processes or IT-budget planning. Thus, our study, as well as the studies referred to above, may be regarded as work that does in fact show the SME context, which may further help the security community address the gaps related to cybersecurity awareness and practices of SMEs.

7 CONCLUSION

The contribution of this paper is a survey based on responses collected from 141 SMEs based in the UK. The overall objective with the survey is to obtain information about the level of cybersecurity awareness and cybersecurity practices of SMEs.

From a cybersecurity awareness perspective, our results show that the participants perception about their own cybersecurity awareness is rather more optimistic than it should be, and even more optimistic when assessing the level of their SMEs' awareness. Very few (27 out of 141) offer cybersecurity awareness training for their employees, and those who do offer training typically conduct it once a year. It is, however, encouraging to see that a variety of SMEs are trying and adopting some form of cybersecurity training. Despite the expressed concern about cyber attacks (85 out of 141 responding ”moderate” or ”a lot” of concern about possible attacks), there is a lack of cybersecurity culture (121 out of 141 report that they discuss cybersecurity ”not at all” or ”sometimes”). Only about 1/3 (45 out of 141) SMEs report that they have positions dedicated to cybersecurity, and only 21 out of 141 are aware of any previous cybersecurity attacks their company have been exposed to.

From a cybersecurity practice perspective, we see that the most common defences used are anti-virus software, firewalls, access control, software updates, and ensuring appropriate configuration for security on all devices and software. These were used by about 2/3 of the SMEs. However, stronger security measures such as 2-factor authentication, encrypted storage data, encrypted communications, intrusion detection, bandwidth management, and staff security training were applied by less than 1/3 of the SMEs. Despite that most of the SMEs cannot tolerate a downtime of their critical applications more than one day, barely any of the SMEs use tools or have processes in place to assess cybersecurity risks they are exposed to, identify potential vulnerabilities that may be exploited by an adversary, and identify cybersecurity attacks.

Maintaining a high level of cybersecurity awareness and implementing all necessary cybersecurity practices are difficult tasks for SMEs. However, we see that some SMEs do try to stay tuned. We believe our findings provide to the cybersecurity community a better understanding of the SME context in terms of cybersecurity awareness and cybersecurity practices, and may be used as a foundation to further develop appropriate tools and processes to strengthen the cybersecurity of SMEs.

ACKNOWLEDGEMENTS

This work has been conducted as part of the CyberKit4SME project, which is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 883188.

REFERENCES

Bada, M., Sasse, A. M., and Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*.

DCMS, Ipsos MORI (2021). Cyber Security Breaches Survey 2021. https://shorturl.at/chRST. Online, accessed: 2022-09-29.

ENISA (2021). Cybersecurity for SMEs: Challenges and Recommendations. https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes. Online, accessed: 2022-12-16.

Erdogan, G., Hugo, Å., Álvarez Romero, A., Varano, D., Zazzeri, N., and Žitnik, A. (2020). An approach to train and evaluate the cybersecurity skills of participants in cyber ranges based on cyber-risk models. In *Proc. 15th International Conference on Software Technologies (ICSOFT'20)*, pages 509–520. SCITEPRESS.

Erdogan, G., Álvarez Romero, A., Zazzeri, N., Žitnik, A., Basile, M., Aprile, G., Osório, M., Pani, C., and Kechaoglou, I. (2021). Developing cyber-risk centric courses and training material for cyber ranges: A systematic approach. In *Proc. 7th International Conference on Information Systems Security and Privacy (ICISSP'21)*, pages 702–713. SCITEPRESS.

European Commission (2016). User guide to the sme definition.

Gafni, R. and Pavel, T. (2019). The invisible hole of information on smb's cybersecurity. *Online Journal of Applied Knowledge Management (OJAKM)*, 7(1):14–26.

Heidt, M., Gerlach, J. P., and Buxmann, P. (2019). Investigating the security divide between sme and large companies: How sme characteristics influence organizational it security investments. *Information Systems Frontiers*, 21(6):1285–1305.

Hoppe, F., Gatzert, N., and Gruner, P. (2021). Cyber risk management in smes: insights from industry surveys. *The Journal of Risk Finance*.

Khan, M. I., Tanwar, S., and Rana, A. (2020). The need for information security management for smes. In *2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)*, pages 328–332. IEEE.

Lewis, R., Louvieris, P., Abbott, P., Clewley, N., and Jones, K. (2014). Cybersecurity information sharing: a framework for information security management in uk sme supply chains. In *Proceedings of the European Conference on Information Systems (ECIS) 2014, Tel Aviv, Israel*, pages 1–15.

Ncubukezi, T., Mwansa, L., and Rocaries, F. (2020). A review of the current cyber hygiene in small and medium-sized businesses. In *Proc. 15th International Conference for Internet Technology and Secured Transactions (ICITST'20)*, pages 1–6. IEEE.

Paek, H.-J. and Hove, T. (2017). Risk perceptions and risk characteristics. In *Oxford research encyclopedia of communication*. Oxford University Press.

Pugnetti, C. and Casián, C. (2021). Cyber risks and swiss smes: an investigation of employee attitudes and behavioral vulnerabilities.

Raineri, E. M. and Resig, J. (2020). Evaluating self-efficacy pertaining to cybersecurity for small businesses. *Journal of Applied Business & Economics*, 22(12).

Roy, Mekhala (2021). Cybersecurity tops list of SMB priorities as attacks continue. https://shorturl.at/efkn4. Online, accessed: 2022-09-29.

Saleem, J., Adebisi, B., Ande, R., and Hammoudeh, M. (2017). A state of the art survey - impact of cyber attacks on sme's. In *Proceedings of the International Conference on Future Networks and Distributed Systems (ICFNDS'17)*. Association for Computing Machinery.

Senarathna, I., Yeoh, W., Warren, M., and Salzman, S. (2016). Security and privacy concerns for australian smes cloud adoption: Empirical study of metropolitan vs regional smes. *Australasian Journal of Information Systems*, 20.

Sheeran, P. and Webb, T. L. (2016). The intention–behavior gap. *Social and Personality Psychology Compass*, 10(9):503–518.

Smerecnik, C. M., Mesters, I., Candel, M. J., De Vries, H., and De Vries, N. K. (2012). Risk perception and information processing: The development and validation of a questionnaire to assess self-reported information processing. *Risk Analysis: An International Journal*, 32(1):54–66.

Vakakis, N., Nikolis, O., Ioannidis, D., Votis, K., and Tzovaras, D. (2019). Cybersecurity in smes: The smart-home/office use case. In *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, pages 1–7. IEEE.

Von Solms, R. and Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, 38:97–102.

Wilson, M., McDonald, S., Button, D., and McGarry, K. (2022). It won't happen to me: Surveying sme attitudes to cyber-security. *Journal of Computer Information Systems*, pages 1–13.

Witte, K. and Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health education & behavior*, 27(5):591–615.

Yamin, M. M., Katt, B., and Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security*, 88:101636.