**It won't happen to me: Surveying SME attitudes to cybersecurity**

**Martin Wilson, Sharon McDonald, Dominic Button and Kenneth McGarry**

**Abstract**

We report an online survey of 85 U.K-based SMEs that explored their threat and coping appraisals towards five common types of cyber-attack: Network being hacked; Data being stolen or encrypted; malware infection; mobile devices being compromised; and phishing email attack. Overall, SMEs’ reported assessment of the risk of an attack was low, particularly for the possibility of their business network being hacked or their data being stolen or encrypted. However, there was an incongruence in their Threat Appraisals since, while they believed the risks to be low, they reported that the impact would be high. In terms of Coping Appraisal, respondents indicated that measures to prevent such attacks were both inexpensive and effective. However, their reported self-efficacy was significantly lower for keeping mobile devices safe and avoiding phishing attacks. We discuss these results taking into consideration additional qualitative data and provide recommendations for SME engagement.

**Keywords**: SME Cyber Security, Threat Appraisal, Coping Appraisal

**Introduction**

The importance of Small and Medium-Sized Enterprises (SMEs) to the global economy is widely recognized1; so too is their growing vulnerability to cybersecurity attacks2. According to the 2021 UK Government’s cybersecurity breaches survey3, of 1419 businesses, 39% of micro and small organizations were attacked at least once per week. Previous research studies report that SMEs tend to underestimate their vulnerability to cyber-attacks despite, in some cases, understanding the risks involved4–7. However, such vulnerability assessments are often derived from a more generalized notion of cyber threats rather than being tied to specific, common, types of threats.

The work presented in this paper was spearheaded by the North-East Business Resilience Centre (NEBRC). A not-for-profit partnership between policing, academia and the private sector whose aim is to assist SMEs to become more resilient to fraud and cybercrime. The NEBRC wanted to understand SMEs’ attitudes to cybersecurity adoption and whether SMEs believed they were vulnerable to specific types of threat (e.g., phishing, network hack etc.). This baseline understanding would be used to target the NEBRC’s ongoing work with the sector to debunk misconceptions and provide targeted help and support to the SME community.

The current study presents the results of a survey that explored SMEs’ perceptions of cybersecurity. The study builds on previous research by examining SME attitudes regarding the most common cyberattacks and their perceived ability to take preventative steps against such attacks. Understanding SMEs’ threat and coping appraisal to different types of cyber threats will enable us to identify interventions that may help SMEs build better cybersecurity practices.

Before describing our approach and results we, briefly, review the existing literature on SME engagement with cybersecurity.

**SME attitudes to cybersecurity adoption**

Few studies have sought to gauge SMEs’ attitudes towards cybersecurity. The paucity of research may be due, in part, to the reticence shown by SMEs to engage with researchers4. Surveys report low response rates despite the best efforts of the researchers involved8. Our evaluation of the literature suggests that the following factors may be significant in SME cybersecurity engagement or, indeed, the lack thereof.

**Optimistic risk appraisals**

Several studies highlight that SMEs report optimistic risk appraisals about the likelihood of a cybersecurity attack4,7,9. For example, from a survey of 110 Scottish SMEs, Renaud and Weir7 report that SMEs do not take cyber threats seriously, with 52% of participants believing cybercrime posed little risk. Furthermore, only 15% had an accurate risk appraisal, and very few implemented cybersecurity protective measures.

The reasons for SMEs’ optimistic risk appraisals include size and turnover6. Some SMEs believe their actions are sufficient because they have not experienced an attack10 or that they are too small and insignificant to be attacked9. Both misperceptions may lull SMEs into a false sense of security and they may also lead them to undervalue their data11.

That SMEs underestimate the risk of an attack is unsurprising. When faced with an unpalatable truth that we might face some form of harm through our actions, or inactions, people will, strive to reduce the resulting cognitive dissonance that arises when our behaviors and thoughts do not align. For small concerns, a lack of action may not be born out of a lack of will to act, but more from a lack of resources to be able to act7. Given that tension, SMEs will undoubtedly engage in strategies to reduce dissonance. McGrath12 outlines several dissonance reduction strategies. These include:

*Distraction* *and forgetting* – we distract our attention from the dissonant thoughts to avoid the negative affective they create. If we are distracted for long enough, we forget the dissonance arousing factor. Distraction may be relatively easy for a busy SME owner who may be fulfilling several roles within their organizations.

*Adding consonant cognitions* – we add additional cognitions or thoughts that concur with our behavior by finding information that supports our position. For example, SMEs may use the tendency of the media to report cybercrime in large organizations to add the consonant cognition that cybersecurity is an issue for national and multinational companies.

*Trivialization* – we trivialize the inconsistency, thereby reducing its importance. For example, SMEs might trivialize by concluding their data assets are worth little therefore the impact is of little consequence.

*Denial* – we may simply deny the possibility of the risk altogether.

The most difficult way to reduce dissonance is to bring attitudes and behaviors into alignment. For cybersecurity adoption, this is a complex problem. There is the issue of perceived costs plus the lack of an immediate and tangible return on investment. Moreover, cybersecurity is difficult for non-experts to understand; it has its own lexicon that is impenetrable for the average person. Indeed, lack of knowledge and understanding are identified as being clear barriers to cybersecurity engagement4.

**Action, knowledge and understanding**

The ever-changing nature of the cybersecurity threat landscape means that without continued attention to their defenses, SMEs may feel that they are protected when they are, unwittingly, exposed. In a survey of 370 small businesses in the USA, Berry and Berry13 found that (74%) reported using protective measures such as antivirus software. However, less than half of those kept pace with software updates; thereby reducing the protection offered. Similarly, Valli, Martinus and Johnstone14 surveyed 50 Australian SMEs finding that 40% reported employing ineffective countermeasures. Mobile technology was reported to be the dominant platform for these SMEs, but they demonstrated poor knowledge of smartphone security meaning that their mobile devices were extremely vulnerable to attack.

**Resource barriers**

Renaud and Weir7 highlight the cost of cybersecurity as a key barrier for SME engagement. SMEs frequently lack the resources to either fund in-house security expertise or to pay for external consultants. In-house expertise appears to be a key determinant for the successful adoption of information security measures such as GDPR preparedness15. However, external expertise and even free advice may be viewed with suspicion. Renaud and Weir7 report SMEs lack trust in government advice regarding cybersecurity.

SMEs face a myriad of competing demands. It is, therefore, no surprise that time is another limiting factor cited by SMEs6. When faced with a choice, SMEs will likely prioritize other business-critical functions such as raising finance ahead of cybersecurity.

**Human Factors**

Human factors issues are referenced by several researchers 4,5,16,17. These included the relationship between an individual’s role in the business and their attitudes to cyber-security. For example, Barlette et al.,5 surveyed 292 French SMEs and found that for business owners, the primary driver to adopt security measurers was social influence factors, such as comparing their current security practices to those of competitors/partners. Whereas non-owner Chief Executives, were more influenced by their ability to cope with and or avert the threat.

Other issues related to compliance, policies and training. Poor information security behaviors demonstrated by employees can be an open door for hackers4,17. Therefore, it seems reasonable to conclude that the implementation of training and information security policies within SMEs should be a priority. However, research studies suggest that SMEs are behind the curve. For example, Berry and Berry13 surveyed 370 small businesses in the USA about their approach to risk management and cyber threats and found that only 6.5% reported having written security policies.

A written information security policy may serve to establish an organization’s expectations vis-à-vis employee behavior, which can be reinforced through appropriate training. However, as Gundu16 points out, knowledge and behavior do not always align. In an action research study with 30 employees from a South African SME, Gundu16 found that reported behavioral intention following cybersecurity awareness campaigns was high (85%) however, the employees’ actual reported behavior scores were low (54%).

**The present study**

The present study explores SME attitudes to the most common type of cyberattacks and their perceived ability to take preventative steps against them. This builds on previous work which has profiled SMEs’ attitudes towards cybersecurity threats in general. The understanding generated by our study may be beneficial in helping organizations to provide tailored support to SMEs in those areas where the knowledge-action gap is demonstrably low but the potential for attack is high.

**2.0 Methodology**

In this section, we describe the design, piloting, and implementation of our web-based survey. At the end of this section we present our research hypotheses.

* 1. **Survey Question Design**

Our survey was inspired by two sources: the behavioral models that have been previously used to examine cyber-security adoption18 and the types of attacks that SMEs face coupled with the response measures they might adopt to defend against those attacks as identified in the National Cybersecurity Centre’s (NCSC) guidance for small business19.

In the section that follows we explain how these sources were used in the design of our survey and present the questions that we used.

* + 1. **NCSC Small Business Guide**

The NCSC Small business guide was used to identify specific types of threat and responses to those threats. The following areas were identified:

* implementing data backups
* keeping mobile devices safe
* preventing malware damage
* avoiding phishing attacks
* using passwords to protect data

**2.1.2 Use of Behavioral Models**

Behavioral models have been used to help us to understand the relationship between behavior and intended action. These models generally hypothesize that our attitudes and/or beliefs will lead to subsequent behaviors.  As such, the models are founded upon both cognitive and affective factors which, when combined, may determine protective behavior.

One model that is at the forefront of attention concerning cybersecurity is Protection Motivation Theory (PMT)18. The basis of PMT is that fear, delivered through messages or “fear appeals”, triggers threat and coping appraisals which motivate people to change attitudes and behaviors20. Although PMT was a source of inspiration for our questions, we did not set out to test this model. Our purpose was to use some of the constructs from the models to explore SME attitudes. We adopted the following constructs from PMT.

**Threat Appraisal:** the individual assessingthe risk of the event or consequence happening to them (*perceived vulnerability)* and the perceived seriousness of the threat if it did occur (*perceived severity).*

**Coping Appraisal**: the individual’s assessment of their ability to perform the action(s) that may prevent the unwanted outcome (*Self-efficacy);* the individual’s assessment of the effectiveness of that action in preventing the unwanted outcome (*Response Efficacy)* and the individual’s assessment of the cost of acting (*Response Cost).*

We also wanted to understand the perceived barriers to taking preventative measures. This was achieved through an open free test question where respondents were invited to tell us what they found most challenging about cybersecurity. Finally, we asked our respondents to comment on their engagement with cybersecurity training and their preferences for receiving advice on cybersecurity matters.

Table 1 shows the Likert-scale questions that were used within our survey. These were inspired by Claar21 and Ng et al22.

=================

**Table One about here**

**=================**

Combining the guidance from NCSC and our analysis of the behavior models and the existing literature on cybersecurity and SMEs we derived several hypotheses.

**Hypotheses**

**Perceived Vulnerability (PV):** In line with previous studies 4,6,7, we expect PV assessments will be low for all scenarios with the exception of phishing due to its prevalence 3.

*H1: Perceived Vulnerability assessment will be significantly higher for phishing compared to all other attack scenarios.*

**Perceived Severity:** SMEs will likely know the consequences of a cyber-attack may be severe given the coverage of incidents in the media7. Given recent estimates of the cost of a breach being in the region of £8,460 - £13,4003 and the notoriety around GDPR legislation, we anticipate data loss will be rated as more severe than other scenarios.

*H2: Perceived severity ratings will be uniformly high, but data loss will be rated significantly higher than other attacks*

**Response Costs:** Perceived affordability of cybersecurity measures is reported as low7. We anticipate that cost rating will be affected by the extent to which measures are readily applicable or easy to implement by users with ratings for password control higher than all other measures.

*H3: There will be a difference in the assessment of costs with creating strong passwords being rated as the most cost-effective measure*

**Response Efficacy:** We expect that ratings will be uniformly high in that respondents will be unlikely to gainsay published guidance. However, we anticipate response efficacy will be lowest for phishing because it may depend upon the compliance of others.

*H4: Response Efficacy ratings will be significantly lower for phishing than other attacks.*

**Self-Efficacy**: Previous studies report low SME self-efficacy 7,16,23. Given that the guidance used within the NCSC small business guide presents relatively easy to adopt measures we anticipate that ratings will be uniformly high with exception of phishing avoidance which may rely upon the compliance of others16.

*H5: There will be a difference in ratings for self-efficacy across the 5 preventative measures with efficacy in dealing with phishing attacks being lowest and those relating to passwords being highest.*

**2.2 Survey Piloting and Administration**

The survey design and questions were subject to iterative review within the research team and two separate rounds of piloting with 15 people drawn from cybersecurity professionals, SME owners, and cybersecurity researchers. Different respondents were used in each round.

The survey was tested for usability across a range of devices (mobile, desktop and tablet). We kept the survey short, with an estimated completion time of 8 minutes, to improve response rates24. An ethics statement with informed consent was included at the start of the survey and our research was approved by our university ethics committee.

**2.2.1 Sampling and Dissemination:** We considered the use of random sampling. However, previous studies have achieved poor response rates. Osborn and Simpson8 achieved a response rate of <1% through standard random sampling procedures. We therefore leveraged connections within the NEBRC network and disseminated the survey using Qualtrics to SMEs across England, Scotland, Wales and Northern Ireland. No incentives were offered to complete the survey.

**Results**

The analysis that follows is based upon 85 completed surveys. Following a summary of our respondents’ characteristics we present our analysis of Threat and Coping Appraisal. We then present our data on SMEs’ advice and training preferences. Finally, we discuss our qualitative data.

**Respondent Characteristics**

Table 2 presents the primary characteristics of our sample. Most respondents reported representing Micro Businesses in sectors other than I.T. The majority of respondents were business owners or partners and were based within the Northeast England and Yorkshire regions of the UK.

=================

**Table Two about here**

**=================**

**Threat Appraisal**

Our analysis separately compared each respondent’s ratings for perceived vulnerability and perceived severity on the 5 attack scenarios (phishing, network hack, malware attack and mobile). A Friedman’s test was used as the non-parametric equivalent of a repeated-measures ANOVA because our data is ordinal. Where a significant difference was found we conducted pairwise comparisons using the Wilcoxon test with a Bonferroni adjustment to control for a familywise error. We do not use any grouping variables such as SME size due to unequal group sizes.

**Perceived Vulnerability**

There was a significant difference between the ratings for each attack scenario ( = 83.47, df=4, *p*<.001). Table 3 presents the results for the pairwise comparisons from the lowest-rated scenario (least likely) to highest rated (most likely). Those results marked with an asterisk were statically significant.

=================

**Table Three about here**

**=================**

Respondents reported feeling least vulnerable to network hack (Mdn 2.0, *x̅* 2.54) and data loss (Mdn 3.0, *x̅* 2.66). While not significantly different from each other, both scenarios were rated as being significantly less likely than Malware Infection (Mdn 3.0 2.0, *x̅* 3.04), Mobile device security (Mdn 3.0, *x̅* 3.15), and Phishing (Mdn 3.5.0, *x̅* 3.55). Phishing and Mobile device security received the highest vulnerability ratings, although they were not significantly different from one another.

**Perceived Severity**

There was a significant difference between the ratings for each of the attack scenarios ( = 20.67, df=4, *p*<.001). There was one significant pairwise comparison (Z=-3.345, *p*<.001), between the highest-rated scenario (data loss; Mdn 4.0, *x̅* 3.86) and the lowest (Mobile security Mdn 4.0, *x̅* 3.26).

**Threat Appraisal Summary**

Fig 1 shows the proportion of respondents who rated their Perceived vulnerability and Severity to be low (rating 1-2), medium (rating 3) or high (rating 4-5) for network hack and data loss. In both cases, the risk is assessed as low (dashed outlined circles) but the impact is assessed as high (jagged circle). Ratings for the other scenarios were more congruent with respondents rating the risk of an attack as higher and the impact as equally high.

=================

**Figure one about here**

**=================**

**Coping Appraisal**

In this section, we present our analysis of SMEs’ ratings for Response Costs, Response Efficacy and Self-Efficacy concerning implementing measures relating to the NCSC small business guide recommendations. Our analysis was conducted using the same process as described for Threat Appraisal.

**Response Cost**

There was a significant difference between the ratings for each of the NCSC factors in terms of perceived cost (= 110.67, df=4, *p*<.001). Table 4 shows the pattern of significant differences obtained from pairwise comparisons, the NSCS factors are presented in order of lowest perceived cost to highest.

=================

**Table Four about here**

**=================**

Creating strong and unique passwords (Mdn 1.0, *x̅* 1.54) was rated as being significantly lower cost than making backups (Mdn 2.0, *x̅* 2.45), Mobile security (Mdn 3.0, *x̅* 2.55), Phishing (Mdn 3.0, *x̅* 2.60) and Malware (Mdn 3.0, *x̅* 3.09). Malware prevention was perceived to be the costliest activity and was rated significantly more costly than all other preventative measures.

**Response Efficacy**

There was a significant difference between the ratings for each of the NCSC factors in terms of Response Efficacy (= 37.61, df=4, *p*<0.001). Table 5 shows the pattern of significant differences obtained from pairwise comparisons, the NSCS factors are presented in order of highest rating value to lowest.

=================

**Table Five about here**

**=================**

Maintaining regular backups (Mdn 5.0, *x̅* 4.36), using strong passwords (Mdn 4.0, *x̅* 4.35) and preventing malware (Mdn 4.0, *x̅* 4.22) were rated equally highly with no significant difference between them. Mobile security (Mdn 4.0, *x̅* 3.83) was rated as least beneficial with ratings significantly lower than maintaining back-ups, using strong passwords and malware prevention. Phishing prevention (Mdn 4.0, *x̅* 4.12) was rated as significantly less beneficial than maintaining backups but was not rated significantly different from any other factor.

**Self-Efficacy**

There was a significant difference between self-efficacy ratings for each of the preventative measures (= 66.6, df=4, *p*<0.001). Table 6 presents the results of pairwise comparisons.

=================

**Table Six about here**

**=================**

Respondents reported greater self-efficacy in their ability to use strong passwords (Mdn 5.0, *x̅* 4.29) than any other measure: backups (Mdn 4.0, *x̅* 4.02), Malware prevention (Mdn 4, *x̅* 3.66); phishing (Mdn 4.0, *x̅* 3.29) and Mobile Security (Mdn 3.0, *x̅* 3.16).

They also rated their ability to take regular backups significantly higher than malware prevention, avoiding phishing and keeping mobiles secure. In turn, their ability to deal with Malware was reported as higher than phishing and keeping mobiles secure. There was no difference between the two lowest rated activities: avoiding phishing and keeping mobiles secure.

**Coping Appraisal Summary**

Figure 2 summarizes the scores for Coping Appraisal for each of the 5 NCSC recommendations. Specifically, this figure shows the proportion of respondents’ rating, Response Costs to be low (1-2), their Self-efficacy and Response Efficacy to be high (4-5). Mobile security and Phishing Avoidance have reasonable cost ratings, respondents indicate that measures may be effective, but their reported efficacy is much lower.

=================

**Figure Two about here**

**=================**

**Advice, Knowledge and Training**

Regardless of company size, 48% (n= 41) of respondents reported participating in cybersecurity training in the last year. However, 45% (n=38) reported having no form of cybersecurity training at all. Of this group, 71% (n=27) were Micro businesses, 21% (n=8) were small and 8% (n=3) were from Medium-sized businesses.

**Acquiring cybersecurity knowledge and advice**

Figure 3 presents the range of resources our respondents reported using to gather information about cybersecurity by business size. Overall, 68% (n=58) indicated they relied upon their own learning; 28% (n=24) reported using consultants; 13% (n=11) reported using in-house IT. Other sources of information included: friends (n=2); the police (n=2) bodies such as the NCSC/NEBRC (n=4), online training resources (n=1). Two respondents commented that they do not look for information or advice.

=================

**Figure Three about here**

**=================**

Micro companies reported that they relied more on their own research and less on external and in-house expertise. Larger businesses relied more on the services of paid consultants and in-house expertise. In terms of the number of sources of information used 79% (n=67) reported that they relied on 1 source of information (primarily the web), 17% (n=14) on 2 sources, 2% (n=2) on 3 sources.

**Preference for advice and barriers to advice.**

Table 7 presents the overall ranking for these items with Rank 1 being most preferred/important to Rank 5 being least preferred/important.

=================

**Table Seven about here**

**=================**

**Qualitative Data**

The final survey question asked respondents about their cybersecurity challenges. This question was not mandatory; hence the number of respondents (n=55) is different to the previous analysis. Free-text comments were analyzed using an open card sort technique24.

**Coding Process and reliability assessment**

The second author segmented the free-text comments into discreet units that represented a single concept. This resulted in 69 individual text units that were printed on index cards. One-by-one the second author read each card and attached a Post-it™ note containing a summary label. Cards on the same topic were grouped and these groupings were given thematic labels. Large groups were coded into subthemes using the same process. As a measure of coding reliability, the second author recoded the 69 individual text cards after a period of three weeks had elapsed. Cohen’s Kappa (0.88) was calculated demonstrating excellent reliability.

**Qualitative Themes**

Table 8 presents the five major themes.

=================

**Table Eight about here**

**=================**

**Limited Understanding**

This large theme contained several sub-groupings:

***General lack of understanding:*** 9 comments were made about a basic lack of understanding about cybersecurity. Some respondents (n=5) highlighted that their busy schedules prohibited them from acquiring the necessary knowledge to make decisions about cybersecurity: *“I don't understand it and don't have the time to learn”; “just another hassle”* Others, appeared to believe that they would never reach and adequate understanding: *“it’s beyond me”(*n=4*).*

***Threat landscape*:** 14 comments were made about the challenges of understanding the changing threat landscape. One respondent commented: *“The unknown unknows”*. Another echoed this comment: *“Knowing where attacks are coming from and how to spot them*. Respondents also highlighted their lack of understanding of how cybercriminals operate: *“I don't understand how criminals can access my accounts”* and the recognition that this is constantly changing “*just keeping up to date with all the different methods that criminals are using*”. Staying up-to-date and the new learning this involves was highlighted by 10 comments, for example, one respondent stated: “*it’s hard keeping abreast of constantly changing guidelines and technologies*”

***Appropriate Advice****:* 5 comments were made about the challenges of understanding what their business needs from cybersecurity and the difficulties in trusting advice. These comments highlighted the need for help in determining what sub-set of measures they should adopt from a multitude of options: *“Getting to grips with what we must do rather than may do”*. Another commented: *“What’s appropriate for a small business”* A lack of understanding of cybersecurity terminology and jargon was also highlighted by one respondent as a barrier in adopting advice: *“easy to understand advice - we are not the technicians here and the specialists find it hard to speak in non-tech terms”.* Two respondents from Micro businesses commented on trust which appeared to be linked to how their perceived lack of cybersecurity knowledge, and the intangible nature of cybersecurity measures themselves, hinder their ability to find reliable advice. *“How much of this is actually real? There is always someone willing to take money for fixing problems that don't exist”* Another respondent echoed the latter sentiment, about their interactions with cybersecurity business sales: *“The number of 'shiny box' sales staff trying to sell their latest version of snake oil...”*

**Operational Concerns**

Several respondents simply choose to highlight specific technologies or activities that they found challenging. For example, Encryption (n=3); data protection (n=3) firewalls (n=3). Other comments highlighted the trade-offs between security and business needs, E.g.: *“Balancing the need to service client's needs and keeping data secure”*.

**Dissonance Reduction**

Micro Business respondents suggested that despite having an online presence they generally believed themselves to be invisible to cybercriminals and, as such, invulnerable to cyber-attack. One respondent commented: *“I don’t think I would be the victim of an attack as really who knows about me?”* another commented, *“I have a website, but no one is going to bother with me”.* Others linked their perceived lack of visibility to the size of their turnover: *“my turnover is small, and I do not see myself as a target”*. Another respondent suggested cyber-crime was a problem for large organizations: *“We are a small fish in a huge ocean, I think bigger business has more to fear”.* This perceived visibility was often associated with a stated lack of concern.For example, *“therefore…I don’t worry about it”*. As such there is a tentative indication that respondents may think about business visibility as being a determinant of vulnerability rather than vulnerability stemming from them having an internet-connected device.

**Human Factors**

Comments focused on security issues arising from the workforce, mainly concerning phishing. For example, “*Getting staff not to click on suspicious emails*”. This sentiment was echoed by 9 respondents, one of whom solved the problem by denying staff access to the business email accounts: *“I do not allow them access to the business email”.* Another respondent highlighted the pervasive nature of phishing: *“That happens to everyone though not just business owners”.* The link between staff compliance and training was also made: “*reliance on team understanding and implementing appropriate measures”.* Another commented: *“Training staff has been problematic as they decide not to listen to advice given and continue to click suspicious links in emails before asking IT for advice”.* The latter comment implies that staff willfully fail to comply.

**Management Buy-in**

Only medium sized SMEs raised issues in obtaining support from senior executives and managers, highlighting that their warnings about cybersecurity were perceived in a negative light. One commented: *“it feels like we are being seen by top managers as being negative. But we are just being cautious and trying to protect the company*”.

One respondent highlighted the difficulties in maintaining management support after initial investment: *“After installing and improving alarm management across multiple sites I had the CEO ask if we could now stop monitoring and working on the alarm systems*”.

Two respondents suggested the experience of a breach was the catalyst in changing management attitudes: “*I could not get money to improve functional safety management, nothing had ever gone bang! But after an enforcement notice, I got anything I asked for - Lesson learned you need an incident to shift the CEO mindset*”.

=================

**Table Nine about here**

**=================**

**Discussion**

Taken together our results suggest that SMEs underestimate the risk of a cyberattack. Table 9 summarizes our hypotheses and results. Respondents report mobile loss and phishing to be the most likely attack. They report network hack to be the least likely, indicating that they perhaps do not recognize the opportunistic nature of attacks. With qualitative comments suggesting size, turnover and notoriety will have role in who gets attacked.

While the likelihood of an attack was deemed to be low, our respondents acknowledged that all attack types would impact their business operation and rated them all highly in terms of severity with data loss rated highest. In terms of responding to an attack, measures that were simple to deploy and under personal control were rated more positively. Using strong passwords was rated as the most cost-effective scenario. Using strong passwords and maintaining backups were identified as the most effective response measures. The least effective measures were keeping mobiles safe and phishing avoidance.

Respondents reported the greatest self-efficacy in using strong and secure passwords and lowest self-efficacy in keeping mobiles safe and phishing avoidance. Cybersecurity training was not a priority for our respondents and the majority relied upon their own research rather than seeking professional advice. We now discuss these findings in relation to our qualitative data and the existing literature.

**Threat Appraisal**

Overall, and in line with previous studies7,14, our respondents reported optimistic vulnerability ratings. However, our results highlighted differences in the perceived vulnerability to specific types of threats. Respondents reported they believed phishing and mobile security to be the most likely, with network hack and data loss to be the least likely. We anticipated that phishing would be rated as most likely due to its prevalence and that it crosses both home and business spheres. The higher ratings for Mobile security may arise simply because devices we carry with us are at an increased risk.

Turning to severity, respondents rated the severity of each of the 5 scenarios to be high with a median value of 4. Therefore, while the risk was perceived to be low our respondents, nonetheless, acknowledge the impact of an attack should it occur. Although all scenarios were rated highlighly, the severity of mobile security was rated significantly lower than the highest rated scenario of data loss. Taking perceived vulnerability and perceived severity together there is a basic incongruence in respondents’ ratings for network hack and data loss. Both of these attacks were rated as being unlikely but their impact, if they were to happen, was rated as being high.

The low vulnerability and high severity ratings suggest a gap between knowledge and action previously observed by Gundu16. So, what might account for this discrepancy? Costs would be an obvious mediating factor and we will return to this in our discussion of coping appraisal. For the moment, however, our qualitative data may be able to provide some insights from the emergent theme of “Dissonance Reduction”. Within this theme, there was some indication that despite acknowledging the potential impact, respondents were engaging in dissonance reduction through trivialization, denial and the addition of additional consonant cognitions *“I have a website, but no one is going to bother with me”; “My turnover is small and I do not see myself as a target”; “I doubt hackers would know what data I keep”.* Therefore, some respondents seemed to believe that their size made them invulnerable to hackers despite their dependency on I.T. Indeed, there was a belief that cybercrime was a matter for large organizations with more capital and reputation *“I think bigger business has more to fear*” and that financial loss was a matter for the banking sector: *“they took money, but I got it back from the bank within a day. It's the banks that need to worry about this”.*

Our qualitative data exposed a key misconception about how cyber-criminals operate that must be challenged if we are to tackle SME cyber-security behaviors. Our data suggest that respondents believed that cyber-attacks are generally targeted at a specific business, rather than being untargeted or scattergun in their nature. Osborn and Simpson8 suggest that a lack of knowledge about the nature of cyber-attacks among SMEs leads them to miscalculate the risk.

**Coping Appraisal**

To assess coping appraisal, we asked our respondents to rate the costs, benefits, and their self-efficacy to implement the 5 recommendations of the NCSC small business guide. In terms of resource costs, our respondents rated malware prevention as the costliest item because it involves resource outlay in terms of software purchase. The other preventative measures were rated low in terms of cost; demonstrating that they were within the grasp of a small business and could be achieved via personal vigilance (e.g., using strong passwords). In terms of Response Effectiveness, our respondents indicated all actions were effective, with median ratings of 4. The most beneficial was regular backups and using strong passwords. Least beneficial was protecting mobile devices; although this was still rated highly. Self-efficacy, ratings were high overall, but our respondents rated their ability to use strong passwords higher than any other measure. Self-efficacy in the application of mobile security measures was rated lowest with a median of 3, suggesting at best participants were unsure of their ability to engage in this activity. This supports Valli, Martinus and Johnstone14 who reported that SMEs lacked the necessary knowledge to deal with mobile security.

While our sample rated the response costs as low across all five scenarios, when we asked respondents to rate five primary barriers to cybersecurity cost came out as the primary limiting factor. Our qualitative data suggest that cost becomes a factor when it involves the SME interacting with a third party such as independent cybersecurity specialists which was perceived to be expensive. Respondents expressed concerns about how their lack of cybersecurity knowledge could mean they have difficulty determining the level of support needed *“Getting to grips with what we must do rather than may do”* and that their lack of knowledge but a desire for peace of mind could leave them vulnerable to exploitation from unscrupulous consultants: *“The number of 'shiny box' sales staff trying to sell their latest version of snake oil”*. Respondents clearly articulated the need for advice to match the business needs, highlighting that they need to know what they *should do* rather than what they *could do.*

**Knowledge, training, and advice**

In line with Renaud and Weir7,the majority (68%) of our respondents relied on their own research and learning from the internet (primarily) about cybersecurity with only 28% paying for the services of expert consultants, and only 5% (n=4) reporting that they used free advice from NSCC. This finding is worrying given the potential for discovering misinformation or conflicting findings from web sources. Take-up of training was reported as low with 45% reporting they had never engaged in any form of cybersecurity training. In terms of receiving advice, our respondents reported that they would prefer to receive pre-recorded advice that they can watch and digest at their own pace focusing on practical “how-to” advice that the average lay-person can understand: *“easy to understand advice - we are not the technicians here and the specialists find it hard to speak in non-tech terms”.*

**Recommendations**

We suggest the following recommendations for engaging with SMEs with cybersecurity.

1. **Challenge the misconception about the nature of cyber-attacks**. SME comments about the protection their small size and turnover provide coupled with the low vulnerability ratings for Network Hack, suggest that SMEs believe that are tacks are targeted rather than untargeted. Therefore, awareness training and other engagement materials need to emphasize the opportunistic nature of these attacks.

1. **Support better risk appraisals.** SMEs need to be supported to make more accurate risk appraisals. Education is part of this process but software tools that enable SMEs to profile their IT dependency to garner a more personalized risk assessment may help enable better conversations with providers.
2. **Targeted interventions around mobile security and IoT devices.** Our SMEs reported lower self-efficacy about keeping mobiles secure**.** An allied issue is likely to beIoT devices given their prevalence3. IoT may be another target for cybercriminals, and they increase the complexity of cybersecurity as there is a need to secure not just one, but numerous connected devices25.
3. **Provide pre-recorded advice and training** Our SMEs expressed a clear preference for training material that is pre-recorded, that can be engaged with at the point of need and can be referred to as required rather than alternative delivery methods such as face-to-face meetings or web-conferencing.
4. **Provide tailored entry points to advice**. SMEs want advice that is tailored to their needs: understanding what they need to do based on their current and future activities from the myriad of measures they might face. Given that most of our sample reported using their own web-based research, this might mean organizations such as NEBRC or NCSC providing filters to information where SMEs can profile themselves to receive more personalized information.

**Limitations**

A key limitation is the small sample size. However, within this sector this is not uncommon. A challenge for researchers is securing the business community’s engagement. Moreover, the sample was self-selecting and may have been completed by respondents with more interest in cybersecurity. Finally, we assessed the threat and coping appraisal from one question per construct and triangulated this with qualitative data. We could have used a greater number of items. However, our approach was guided by a desire to increase the response rate by reducing the burden of completion and so this compromise was made. Interviews would, no doubt, have revealed more nuanced insights; we are currently conducting a follow-up interview study.

**Conclusions**

Despite their importance to the UK economy and their dependency upon I.T, our findings suggest that SMEs are still discounting their risk of cyber-attack. This is despite knowing that if an attack were to occur the consequences could be significant. Perceptions of vulnerability appear to be tied to the notion that most cyber-attacks are targeted. This is fueled by SME misconceptions about size, turnover, reputation rather than the indiscriminate approaches used by cybercriminals.

However, the news is not all bad. Our survey suggests that our SMEs feel able to action 3 out of 5 preventative measures with their reported self-efficacy waning in respect of phishing avoidance and mobile security. Lower self-efficacy about phishing may be due to the prevalence of phishing attacks or, perhaps, because it is difficult to control the behaviors of others. The latter suggests an area of focus for training and awareness programs. Our qualitative data suggests that as businesses grow or their dependency on technology increases there is a need for further training/knowledge transfer so that SMEs can both garner good advice and understand what actions *should* be taken from the myriad of actions that *may* be taken. SME owners and employees are focused on the day-to-day challenges of operating a private concern. Therefore, while cybersecurity is important, it may always be one step down on a long list of priorities. So too, is engagement with the research community. We are grateful to the 85 respondents who took the time to complete our survey. However, we are mindful that unless researchers can secure the engagement of SMEs, we will continue to struggle to support them.

**Acknowledgements**

We thank the anonymous reviewers for their helpful comments and the NEBRC for their support. Thanks to the SMEs who participated in our research and Alan Lumsden for proofreading the manuscript.

**Declaration of interest**

No potential competing interest was reported by the authors.

**References**

1. Rhodes C. Business statistics, House of Commons Library. 2017;

2. Saleem J, Adebisi B, Ande R, Hammoudeh M. 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. 2017.

3. DCMS, Ipsos MORI. Cyber Security Breaches Survey 2021: Statistical Release. 2021 Mar 24;66.

4. Alahmari A, Duncan B. Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. In: 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). 2020. p. 1–5.

5. Barlette Y, Gundolf K, Jaouen A. CEOs’ information security behavior in SMEs: Does ownership matter? Systèmes d’information & management. 2017;22(3):7.

6. Osborn E. Business versus Technology: Sources of the Perceived Lack of Cyber Security in SMEs. Oxford University Research Archive [Internet]. 2014; Available from: https://ora.ox.ac.uk/objects/uuid:4363144b-5667-4fdd-8cd3-b8e35436107e

7. Renaud K, Weir GRS. Cybersecurity and the Unbearability of Uncertainty. In: 2016 Cybersecurity and Cyberforensics Conference (CCC). Amman, Jordan: IEEE; 2016. p. 137–43.

8. Osborn E, Simpson A. Risk and the Small-Scale Cyber Security Decision Making Dialogue—a UK Case Study. Loukas G, editor. The Computer Journal. 2018 Apr 1;61(4):472–95.

9. Renaud K, Ophoff J. What is Preventing UK SMEs from taking Cyber Security Precautions? 2021; Available from: https://www.muster.scot/docs/MUSTER\_White\_Paper.pdf

10. Renaud K, Ophoff J. A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. Organizational Cybersecurity Journal: Practice, Process and People. 2021;

11. Hayes J, Bodhani A. Cyber security: small firms under fire [Information Technology Professionalism]. Engineering & technology. 2013;8(6):80–3.

12. McGrath A. Dealing with dissonance: A review of cognitive dissonance reduction. Social and Personality Psychology Compass. 2017;11(12):1–17.

13. Berry CT, Berry RL. An initial assessment of small business risk management approaches for cyber security threats. International Journal of Business Continuity and Risk Management. 2018;8(1):1–10.

14. Valli C, Martinus IC, Johnstone MN. Small to medium enterprise cyber security awareness: An initial survey of Western Australian business. CSREA Press. 2014;71–5.

15. Sirur S, Nurse JR, Webb H. Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). In 2018. p. 88–95.

16. Gundu T. Acknowledging and reducing the knowing and doing gap in employee cybersecurity complaince. In: ICCWS 2019 14th International Conference on Cyber Warfare and Security. 2019. p. 94–102.

17. Siponen M, Mahmood MA, Pahnila S. Employees’ adherence to information security policies: An exploratory field study. Information & management. 2014;51(2):217–24.

18. Rogers RW. A Protection Motivation Theory of Fear Appeals and Attitude Change. The Journal of Psychology. 1975 Sep 1;91(1):93–114.

19. NCSC. Small Business Guide: Cyber Security [Internet]. Small Business Guide: Cyber Security. 2020 [cited 2021 Oct 13]. Available from: https://www.ncsc.gov.uk/collection/small-business-guide

20. Shillair R. Protection Motivation Theory. The International Encyclopaedia of Media Psychology. 2020;1–3.

21. Claar CL. The adoption of computer security: An analysis of home personal computer user behavior using the health belief model. All Graduate Theses and Dissertations 878 [Internet]. 2011; Available from: https://digitalcommons.usu.edu/etd/878

22. Ng B-Y, Kankanhalli A, Xu Y (Calvin). Studying users’ computer security behavior: A health belief perspective. Decision Support Systems. 2009 Mar;46(4):815–25.

23. Bougaardt G, Kyobe M. Investigating the Factors Inhibiting SMEs from Recognizing and Measuring Losses From Cyber Crime in South Africa. 2011;14(2):12.

24. Baxter K, Courage C, Caine K. Understanding your users: a practical guide to user research methods. Morgan Kaufmann; 2015.

25. Pal S, Díaz VG, Le D-N. IoT: Security and Privacy Paradigm. CRC Press; 2020.