Extended Abstract

Evaluating Online Cybersecurity Guidance and Support for Small Businesses

Steven Furnell[1], Neeshé Khan[1], Maria Bada[2] and Jason R.C. Nurse[3]

[1] University of Nottingham, Nottingham, UK
[2] Queen Mary University of London, London, UK
[2] University of Kent, Canterbury, UK

{steven.furnell; neeshe.khan1}@nottingham.ac.uk; m.bada@qmul.ac.uk; j.r.c.nurse@kent.ac.uk

Introduction

Cyber security remains a key priority for organizations of all sizes. However, while ensuring appropriate protection is an issue for everyone, it is typically a more challenging prospect for Small and Medium-sized Enterprises (SMEs), with less capability and resources to address it (in terms of both in-house expertise and budget to invest or engage externally).

In the UK, the 2023 Cyber Security Breaches Survey suggested a notable decline in the proportion of SMEs following some basic cyber hygiene practices (DSIT, 2023). Specifically, the 2023 results showed a series of reductions across four key areas when compared to the 2021 findings, as illustrated in Figure 1.

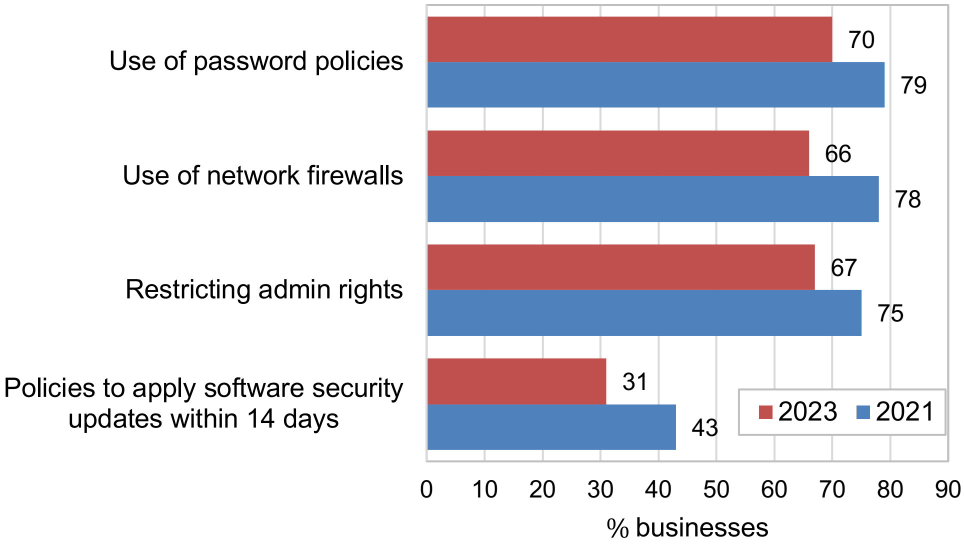

Figure 1: Declining cyber hygiene practices in UK businesses 2021-2023

While the survey does not present a further decomposition based upon the size of the organizations, the accompanying commentary noted that the results observed from large businesses had not changed, and the decrease was particularly amongst micro businesses. This may be indicative of attention towards security being sacrificed in the face of post-pandemic economic challenges and rising costs. However, while shifting priorities can be expected, the consequence for the businesses concerned could nonetheless be unfortunate. Most cyber attacks are opportunistic and based around techniques that basic hygiene measures will help to thwart. Given that SMEs account for a huge proportion of the economy (in the UK and similarly so in other countries), a situation that leaves a greater proportion of them left potentially exposed is a clear cause for concern.

Of course, one of the challenges for most SMEs is that they have relatively limited understanding about what cyber security involves. While good resources are available to help, SMEs may not be aware of them and may not know how to put the advice into practice. For example, the aforementioned Cyber Security Breaches Survey reports that only 15% of micro and small businesses have heard of the UK National Cyber Security Centre's Small Business Guide on cybersecurity (NCSC, 2018).

The CyCOS project

The above concerns have led to the establishment of the CyCOS research project (see www.cycos.org), which aims to enhance the cyber resilience of SMEs by offering a new means to access support around cyber security, and to share lessons and experiences from their peer community.

The initial research is assessing the current situation from the perspective of SMEs seeking cybersecurity support, and from those providing SME-facing advice and support. The SME data collection (conducted via surveys and interviews) seeks to establish their current understanding perceptions and confidence around cybersecurity, as well as their support needs and awareness and use of existing routes available to them. A parallel phase of investigation focuses on the support routes and sources available to SMEs, including the coverage and consistency of support, and the confidence and capacity of those providing it. Following on from these activities, the next phase of the work involves practical capture, tracking and analysis of experiences when cyber security support is sought and provided. Looking from both the SME and advisor perspectives, this encompasses different scenarios (e.g. general guidance, pre-sales advice, post-sales technical support, and support for incident response) and seeks to characterise the resulting 'support journeys' (i.e. from start to finish, including what triggered the need for support, who was contacted, what support was provided, what the outcome was). The resulting case examples will offer insights into aspects such as the skills required to provide support, any challenges encountered, and lessons learned. This in turn will inform the new contribution of the project, which seeks to design and pilot the concept of Cyber Security Communities of Support, as an additional route by which SMEs can seek and receive support from peer organisations (e.g. in the same locality or sector) and expertise from advisors willing to offer their support and guidance in a community context.

The 30-month project is being undertaken in collaboration with a range of relevant supporting partners:

- The ***UK Home Office*** is focused on safeguarding the security and economic prosperity of the UK. As a project partner it has particular interest in understanding the support available to SMEs, and the contribution that can be made by the Cyber Security Communities of Support and will utilise the findings to inform future policy actions.
- ***ISC2*** is a leading international provider of cyber security skills and certification, with over 168,000 certified members worldwide. Alongside expertise to inform activities across the project, ISC2 is contributing free access to its *Certified in Cybersecurity* (CC) training and certification (to enable upskilling of SMEs and advisors participating in the CyCOS pilots).
- The ***IASME Consortium*** is the NCSC's delivery partner for Cyber Essentials (a Government-backed minimum level of cyber security for businesses). IASME offers linkage to the SME community and expertise to guide CyCOS activities and will benefit from the planned promotion and advocacy of the Cyber Essentials standard within the CyCOS.
- Three participating ***Cyber Resilience Centres*** (London, Eastern and East Midlands) support SMEs and third sector organisations reduce their vulnerability to cybercrime. Each offers expertise across the project, leading to direct participation in CyCOS pilots.
- The ***Chartered Institute for Information Security*** (CIISec) is an independent not-for-profit body with over 10,000 members, dedicated to professionalism in cyber security. As a partner, CIISec offers access to SMEs via its corporate partner network and regional hubs, alongside expertise and SME-relevant guidance materials that can feed into the community pilots.

- The ***Centre for the New Midlands*** is an independent, community interest company seeking collaborative solutions to the social and economic challenges in the Midlands. It offers a channel to engage SMEs, and (via its Digital Leadership Board) access to advisory sources and input to inform community design and pilots.

The focus of this paper is around initial insights from the assessment of existing advisory sources that SMEs would encounter if searching for support online. Such guidance is likely to be a natural starting point for many SMEs seeking to understand what they need to know about cybersecurity and what to do about it.

Evaluating guidance from online sources

A series of related sources were identified by means of web search for SME-facing guidance, or by directly visiting sites from providers that SMEs would be expected to know and potentially view as authoritative and credible (e.g. official sources, Internet Service Providers). A series of 17 individual searches were used, examples of which are presented below, along with a Boolean search to see if it identified additional sources. In each case, the equivalent to the first three pages of results were checked, which was considered to be comprehensive on the basis that most users will not typically progress to even the second page of search results (Turner et al. 2021).

Table 1: Examples of searches used to identify online guidance sources

Individual searches	**Boolean string**
cybersecurity guidance for small businesses	[("SME" OR "small business" or "micro business" or "SMB") AND ("Cybersecurity" OR "cyber security" OR "information security" OR "infosec" or "security") AND ("advice" OR "guide" OR "guidance" OR "recommendations" OR "tips")
SME cyber security UK	
how to set up cybersecurity for SME UK	
Cyber security policy for small business uk	
cyber security tips for small businesses UK	
how to cyber secure small business UK	
how to cyber secure medium business UK	
cyber security support for SME UK	
cyber security materials to support SME UK	
cyber security support materials for UK SME	

The search results were then filtered in several stages in order to yield a sample set that would then be analyzed in detail. Firstly, we omitted many results that were simply opinion pieces, blog posts and similar, which left a pool of 72 sources. We also omitted those for which access was behind paywalls or in some other way limited to subscribers (e.g. members of professional organizations), taking the available number down to 44. From the remaining accessible results, we were then seeking sources that were clearly presented as SME-facing guidance and advice. This left a set of 31 relevant sources, each offering information directly identifiable as a small business cyber security guide (or offering 'top tips', 'key advice' or similar).

The resulting sources were then assessed on the basis of three factors of interest:

- **Coverage**: What aspects of cyber security are addressed?
- **Clarity**: Is the guidance provided in using words and terms that SMEs who have little or no technical security knowledge would be likely to understand?
- **Completeness**: How far does the advice/guidance go? Does it simply say 'you need to consider XYZ issues' or does it advise on how to do it, or some middle ground of pointing toward other sources for further support?

The evaluation revealed that the guidance provided was anything but consistent. Table 2 below presents a subset of the findings, taking two sources from each of the provider categories as examples. In each case, the table is indicating whether the guidance included coverage that could be mapped to each of the NCSC's 10 Steps to Cyber Security (NCSC, 2021), as well as whether there was coverage to explain the nature of SME-facing cyber threats more generally. As can be seen, there is a wide variation in what each source is found to cover, and some topic areas tend to receive scant coverage compared to others. Against this backdrop, it would be entirely reasonable to find SMEs coming away with an incomplete and inconsistent information, and thereby potentially remaining confused about what they should actually be doing.

Table 2: Examples of topic coverage from different online guidance sources for SMEs

Category of Provider	Risk management	Engagement and training	Asset management	Architecture & configuration	Vulnerability management	Identity & access management	Data security	Logging and monitoring	Incident management	Supply chain security	Threats
Government			✓	✓		✓	✓				✓
Government		✓	✓	✓	✓	✓	✓				✓
IT body	✓	✓		✓		✓	✓				
IT body		✓		✓	✓	✓	✓		✓		✓
SME body				✓		✓	✓	✓	✓		✓
SME body		✓		✓	✓	✓		✓			
Insurance	✓	✓	✓						✓		✓
Insurance	✓	✓		✓	✓		✓	✓		✓	
Security vendor		✓	✓	✓	✓	✓	✓	✓			
Security vendor	✓			✓	✓	✓	✓				
ISP	✓	✓		✓	✓	✓	✓				
ISP		✓		✓	✓	✓	✓				
IT retailer		✓		✓	✓	✓		✓			
IT retailer	✓	✓		✓		✓					

The clarity and completeness factors were also significantly variable. In terms of clarity, the majority did not define 'cyber security' and half provided steps that were considered difficult to follow. In terms of completeness, a little over a third only offered topic-level advice whilst the length of the guide itself varied across the board. Our assessment therefore suggests that SMEs may find the materials relatively limited, and (despite the naming of various sources referring to offering guides and tips) typically of more use in raising awareness than guiding resulting actions.

Conclusion and Future work

The work to date has already provided a clear indication of the challenging situation that may face SMEs when seeking guidance from online sources. Although they will almost certainly *find* a multitude of sources, the quality and depth of what they locate has significant variability across several dimensions. As such, it is unclear whether SMEs would truly benefit, and there is an active risk of them forming an incomplete picture of what they need to be concerned about.

As the project progresses, the further work will track SME support journeys as they unfold, in order to develop case studies of what works and how to avoid issues. All of the evidence collected from this and the earlier phases will then inform the design and piloting of the Cyber Security Communities of Support themselves.

Acknowledgements

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

DSIT. (2023). Cyber security breaches survey 2023, Official Statistics. Department for Science, Innovation & Technology. 19 April 2023. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023

NCSC. (2018). Small Business Guide: Cyber Security. National Cyber Security Centre. 15 November 2018. https://www.ncsc.gov.uk/collection/small-business-guide

NCSC. (2021). 10 Steps to Cyber Security. National Cyber Security Centre. 11 May 2021. https://www.ncsc.gov.uk/collection/10-steps

Turner, S, Nurse, J. R. C., Li, S. (2021). When Googling it doesn't work: The challenge of finding security advice for smart home devices. Human Aspects of Information Security and Assurance. HAISA 2021. IFIP Advances in Information and Communication Technology, vol 613. Springer, Cham. https://doi.org/10.1007/978-3-030-81111-2_10