It's Not My Problem: How Healthcare Models relate to SME Cybersecurity Awareness

Brian Pickering[1][0000-0002-6815-2938], Costas Boletsis[2][0000-0003-2741-8127], Ragnhild Halvorsrud[2][0000-0002-3774-4287], Stephen Phillips[1][000-0002-7901-0839] and Mike Surridge[1][0000-0003-1485-7024]

[1] University of Southampton, Electronics and Computer Science, IT Innovation, Gamma House, Enterprise Road, Southampton. SO16 7NS, UK;
{j.b.pickering, s.c.phillips, ms8}@soton.ac.uk
[2] Forskningsveien 1, 0373 Oslo, Norway;
{konstantinos.boletsis,ragnhild.halvorsrud}@sintef.no

Abstract. Small and medium enterprises (SMEs) make up a significant part of European economies. They are often described as poorly place to deal with cyber risks though because of resource constraints or commercial interests. Providing appropriate tooling would facilitate a greater appreciation of the risks and provide mitigation strategies. In a series of workshops demonstrating visualization tools for cybersecurity, constructs from healthcare models such as awareness, self-efficacy, and a willingness to engage were investigated to throw light on the likelihood that the technologies would be adopted. Although most constructs were validated, it turns out that self-efficacy could more appropriately be interpreted as a desire to understand a broader company narrative rather than empowering any individual to identify and manage cyber risk. As part of an ongoing examination of technology acceptance, this work provides further evidence that technology must be contextualized to make sense for the individual as part of the SME rather than as individual employee.

Keywords: Cybersecurity awareness; SME; company narrative; qualitative methods; technology adoption; Health Belief Model; Normalisation Process Theory.

1 Introduction

The increasing sophistication of cyber-attacks may have particularly negative consequences for organizations such as small and medium enterprises (SMEs). They are focused on their main business and may not therefore have the resource or expertise to identify and handle such risks. In this study, we investigate the use of constructs from healthcare models specifically conceived in relation to risk awareness and behavioral change in an attempt to understand the willingness of this type of enterprise to engage with cybersecurity tooling.

1.1 The SME Landscape

The risk of cyberattacks for SMEs is well established. Sharma et al. [1] list the types of attack that have been reported, while Bell [2] suggests that SMEs may not have the resource to deal with them. Lewis and his colleagues [3] maintain that while individual threats are significant, an SME as part of a supply-chain presents additional cybersecurity concerns since any vulnerability they display can affect others across the chain. They attempt, therefore, to identify the perceived sensitivity of individual threats in relation to SME willingness to share information about cybersecurity readiness. In his report, Bell [2] focuses primarily on technology vulnerabilities, while Sharma et al. [1] and more recently Vakakis et al. [4] recognize vulnerability associated with individual employee behavior, making them targets themselves [5]. Not surprisingly, Lewis et al. [3] identify training and awareness as important and shareable aspects of cybersecurity status. Further, individuals are not necessarily attuned to cyber risks [6]. So, if people are not aware of appropriate behaviors, we need to understand how to encourage them to change how they act [7]. This is true in all aspects of our lives [8]. However, as the NHS WannaCry attack in the UK illustrates, individual actions and a lack of organizational procedures exacerbate the risk [9].

Understanding personal risk, it has been suggested, is a key motivator to engage with a whole range of preventative behaviors, including models such as the Health Belief Model (HBM) [10-12]. As well as this perception of risk, however, for an intervention to be sustained, patients or users in other domains need to believe the specific intervention will help them to manage the risk. Thus, self-efficacy was introduced in later iterations of the HBM. Taking health interventions as a metaphor for the well-being of the SME, then evidence of the constructs of the HBM in engaging with SMEs in connection with supporting technology might encourage responsibility-taking and behavioural change [7]. This exploratory study seeks to investigate first the levels of cybersecurity threat awareness and then how decision-support technologies might encourage self-efficacy as a precursor of protective behavioural change.

2 Background

Evaluation of new or enhanced technologies is often underpinned implicitly with one of several causal behavioral models. Typically, they seek to predict the intention to adopt based on some situational context, which may include the demographics of the target users, and some other decision criteria. An early broader formulation derives from the Theory of Reasoned Action (TRA) and thence of Planned Behavior (TPB) [REFs]. Significantly, as TRA developed into TPB, the notion of self-efficacy was introduced: those who might be motivated to act in a given way – adopt a technology or change behavior – would believe that adoption would improve their self-belief in achieving a goal.

Focusing specifically on technology at the decision point, Davis [REF Davis, 1985/89] and then Venkatesh [REFs – Venkatesh et al, 2003] tended to focus on characteristics of the technology itself at the decision point and on moderating factors like the context for technology use and the experience of adopters. Quantitative instru-

ments were developed to capture constructs such as the perceived ease-of-use of the technology and the dependent perceived usefulness of the technology. Together or independently, these are assumed to predict the intention to adopt a given technology. Similar models have also been applied to the adoption of healthcare interventions [REFs – Conner & Norman, 2005]. Here the focus is on patient awareness and response to risk (Health Belief Model) or to fear (Protection Motivation Theory).

One of the inherent issues with TPB and similar models, however, is that the decision point leads to an *intention* to behave in a given way, or an *intention* to adopt the technology. The bridge between this intention and the actual behavior is often overlooked. So, conceptual frameworks such as diffusion of innovations (DoI) focus on factors including but not confined to the technology which might predict up-scaling and spread of technology (innovation) beyond the decision point itself [REF].

In our own recent work, we have questioned whether quantifying usability and usefulness can really predict the willingness to adopt technology [REFs]. From our exploratory work, we concluded that potential adopters need to develop an understanding of how the technology can help them or their colleagues specifically with their individual responsibilities. In other words, we found some evidence for the importance of self-efficacy as a construct for technology adoption. Further, in creating narratives around the use of technology, we argued that individuals internalize the potential with the technology to make sense of it in their own context. We report below a specific empirical investigation into the use of visualization tools for cybersecurity. We aimed to explore both the decision point and potential influences for longer term adoption and use.

2.1 Health Belief Model (HBM)

With parallels to TPB, HBM contextualized the decision to adopt a suggested intervention based on constructs related to the context for the intervention, including how it might improve self-efficacy, and perceived individual control [REFs]. A patient for a given intervention would thereby consider their risk regarding a specific condition, such as obesity or contracting an illness, and its likely impact. In addition, the model suggests, they would consider how the proposed intervention might help them address the risks and impacts, and the latitude they have to take action [REF]. This echoes, we maintain, cyber risk awareness and the adoption of technologies like firewalls and anti-virus software [REF Rokkas / Neok, 2020]. Protection Motivation Theory (PMT), which shares structural similarities with HBM, was part of the development of a research model intending to predict the adoption of cybersecurity enhancing behaviors in SMEs [REF: Browne et al, BLED, 2015] where the focus is on coping strategies (or self-efficacy). Warkentin and his colleagues went further to explore long-term cybersecurity aware behaviors based on a contextualized and empirically validated version of PMT [REF Warkentin et al, 2016]. It is such contextualization, they conclude, which is key to longer term adoption of appropriate behaviors.

In a similar vein, we explore the operational context within which SME employees need to identify and implement appropriate actions regarding cybersecurity. We use constructs from HBM because this focuses on the more general *awareness* rather than

specific and individual fear as with PMT. It was felt that awareness might encourage responsibility taking as an employee of the SME.

2.2 Normalisation Process Theory (NPT)

As stated above, even if the intention to adopt technology were to predict its actual adoption, continuing the behavior is a different issue. In addition to constructs of the HBM as they relate to risk and impact awareness around cybersecurity, a supplementary question arises. If SME employees show some appreciation of the risks and potential impact when exploring cybersecurity visualization tools would they also show appreciation that the tools could help them take action to protect against cyber-attacks? Indeed, Warkentin et al [REF] specifically target the continuation of appropriate behaviors in response to the fear, in PMT terms, surrounding a potential attack. Looking at the propagation of innovation in the first instance, perhaps the DoI might throw some light on how technology use may persist. However, and specifically for healthcare again, frameworks have been developed which look at the actual adoption and adherence to an intervention. One such framework is the NPT [REF – May et al, 2009a, 2009b].

Based on extensive empirical investigation, it predicts four main thematic areas which need to be explored, including the user community's buy in to the concept behind an intervention (its *coherence*), its willingness to engage (*cognitive participation*) and to act towards implementation (*collective action*) [REF]. Crucially, the fourth involves continuous *reflexive monitoring*. The other constructs are consistent with the intention to adopt and the initial stages of adoption. The fourth, however, introduces the notion that users should continue to engage and explore technology or intervention benefits and affordances. In NPT terms, would they demonstrate cognitive participation and a willingness to take collective action? Cognitive participation would derive from the awareness signaled with the constructs from HBM. A willingness to take collective action extends HBM self-efficacy and the perceived benefit of the tools into the awareness of personal responsibility for cybersecurity risk mitigation. As May and his colleagues state, these four phases do not necessarily occur sequentially [REF]. We might expect users, therefore, to begin to develop a narrative involving the technology from the early stages of exposure to it as part of cognitive participation which would then lead to collective action: they appreciate where the technology fits and what value it brings, but then see a broader context for its usefulness.

3 Method

This study uses mixed methods to explore SME awareness and attitudes to cybersecurity risk. Constructs from HBM and NPT were used to explore SME employees' awareness of cybersecurity risks and their willingness to adopt appropriate tooling to mitigate such risks. These were validated initially against issues from an independent-

ly developed quantitative instrument aimed at a sample of SME employees. The constructs were then explored during ethnographic observation followed by a more detailed thematic analysis of a series of workshops within the context of a European project looking at providing technical support for cybersecurity.[1]

Table 1. Coding scheme for Thematic Analysis of the workshops

Code	Model	Description
Risk awareness	HBM	Awareness that there is a risk from cyber attacks
Impact awareness	HBM	Awareness of the potential impact of such attacks
Self-Efficacy	HBM	Perceived ability to deal with cyber risks
Benefits of Tool Use	HBM, NPT	Perceived benefit of using tools
Tool Cohesion	NPT	Perception that tools provide a coherent view of risks
Adoption Willingness	NPT	Willingness to adopt and explore the tools
Increase in Understanding	NPT	Expression of increased awareness

3.1 Design

An anonymous online survey had been developed independently based on input from cybersecurity experts when asked to consider what important issues might affect SME risk. It was drafted and run mainly by one of the researchers (CB), independently of the present study and intended to collect SME attitudes and practices regarding cybersecurity through the employee lens. As such, it provides a useful comparison with analyses effected in the present study.

For the qualitative analyses reported here, we had previously investigated the use of qualitative methods in understanding how potential adopters react to technology [13, 14]. A coding scheme was defined in advance based on the main constructs from the HBM and on the phases of the NPT as described above by one of the researchers (BP). The scheme was intended as the basis for analysis of direct engagement with representative SMEs via a series of workshops and was not shared with the other researchers until after the online survey and workshops. It should be remembered that the goal of the workshops was to understand SME business operations *not explicitly* participant awareness about cybersecurity risk.

The coding scheme is summarized in Table 1, including a brief description of each construct. These initial constructs are more typical, of course, for exploring health interventions, including technology. Although we argue that risk awareness regarding cybersecurity commercially might be seen as analogous with health and wellbeing

[1] The work reported here was approved by the Faculty of Engineering and Physical Science Research Ethics Committee (Ref ERGO/FEPS/62067)

awareness individually, some level of validation of these constructs seemed appropriate and was carried out against the results from an independent, anonymous, 24-item online survey[2] and as part of ethnographic observation during the workshops described below.

3.2 Participants

The online survey attracted 164 self-selecting participants recruited via internal networks (an opportunity sample of 23) and a 3rd party (141 from a purposive sample). For the workshops, eight participants from four SMEs engaged with the project took part in the workshops as well as the researchers themselves. Typically, only one researcher moderated the sessions whilst the others attended solely to ask questions or respond to specific points when asked. Participants were not cybersecurity experts, nor did they have any such specific responsibility within their respective organizations.

3.3 Data Collection

The online survey had been launched via an external platform and ran for approximately 3 weeks. The workshops were run over several months, with participants from SMEs across four domains: finance, healthcare, utilities and automotive manufacturing. Participants from a given SME engaged separately, except where an existing relationship existed; a given workshop, therefore, was attended mainly by employees from one SME only. The workshops were organized as an introduction to issues of cyber security and the use of tools to help individuals or the enterprise as a whole understand and manage any such threats [19]. Thirteen workshops lasting over 27 hours in total were recorded across the four domains individually. The objective of the workshops was to understand the operational context for each of the SMEs and were not explicitly intended to explore participant understanding or awareness of cyber risks and mitigation. The second and third workshops involved a focused discussion of cybersecurity, including a demonstration of tools which visualise threats associated with the infrastructure [15] on the one hand, and typical business processes on the other [16]. In the third interview, participants were encouraged to work with the researchers to develop visualisations of their business infrastructure using the tools. Transcripts of the initial workshop for each SME were pseudonymized and checked with participants to ensure accuracy. Transcripts of the remaining workshops were automatically generated, a process which did not preserve identifiers of the original participants. Some ten and a half hours have been analyzed thus far.

[2] https://cyberkit4sme.eu/JustinTimeCybersecurity.html

3.4 Analysis

The online survey had been independently developed on the basis of specific questions felt by cybersecurity experts was compared by one the researchers (CB) against the constructs in Table 1 with the intention of identifying a correspondence between the cybersecurity experts' views and the coding schema. We do not cover all responses to those questions here. In addition, one of the researchers (RH) made field notes during the workshops. These were then compared against the constructs in the coding schema as an initial indication that the issues of awareness, impact and willingness to adopt technology were felt salient.

Finally, after each workshop was recorded and transcribed verbatim, a third researcher (BP) used the coding scheme to carry out a thematic analysis of what participants discussed. This included all constructs from Table 1 and not just those validated in the previous two phases (comparison with the online survey and ethnographic observation).

4 Results

4.1 Cybersecurity coverage (anonymous survey)

The survey indirectly captures SME employee awareness of cybersecurity risks through examining their knowledge of the cybersecurity-related practices in the SMEs they work for. For example, and without detailing all responses, 70% of the responses to *Does your company offer courses or training material for employees to raise awareness about cybersecurity?* said no such education and training was available; while in reply to *Does your company have positions dedicated to cybersecurity at any level?* 60% said *no* and 7% *don't know*; and so forth.

For the rest, Table 2 simply lists the questions compared with a given construct without summary statistics of responses. So, it turns out the survey based on cybersecurity experts' perceptions of what is important for SMEs coincides with the first four constructs of Table 1, namely from the HBM. These are summarized in Table 2.

Table 2. Construct correspondence in the online survey

Code	Description
Risk awareness	Does your company offer courses or training material for employees to raise awareness about cybersecurity? Does your company have positions dedicated to cybersecurity at any level? Do you discuss cybersecurity issues on your company meetings or presentations or, in general, internally in your company?
Impact awareness	To what degree do you fear for a cybersecurity attack towards your company? How long do you think your critical applications and sys-

	tems can be shut down before significant disruption is caused to the company?
Self-Efficacy	How would you characterize your own knowledge about cybersecurity?
Benefits of Tool Use	What security measures is your company taking to avoid cybersecurity attacks? Does your company use specific processes or tools to assess risk to its IT assets? Does your company use specific processes or tools for identifying cybersecurity vulnerabilities? Does your company use specific processes or tools for identifying cybersecurity attacks?

Apart from seeking to address the individual HBM constructs, the survey provided an additional motivation to explore SME employee willingness to adopt appropriate tooling as represented by the NPT-based constructs which had not been possible via the survey.

4.2 Ethnographic observations

Remembering that the intention of the workshops was to gain an understanding of the operational and business environment of the SMEs, observational notes from one of the researchers (RH) were reviewed in regard to the constructs proposed in Table 1.

Table 3. Summary of ethnographic observations

Construct	Observations
Risk / Impact Awareness	Some participants reported frustration that ICT colleagues would not always share knowledge or know-how Some were aware only of the potential for *technical* risks Some were less aware, if at all, of risk associated with employees, such as social engineering attacks or an *evil insider* Notwithstanding who might be responsible for security, many saw regulatory or similar compliance as sufficient to guarantee cybersecurity risk
Self-efficacy	Some SMEs outsource their infrastructure and so lack the awareness and ability to take responsibility for cybersecurity Some reported a lack of communication from the ICT infrastructure provider
Willingness to adopt	Having seen the tooling demonstrated, some expressed enthusiasm for using the kind of tooling demonstrated to enhance their awareness of risk

This analysis is summarized in Table 3 here. As with the coverage of the questions in the anonymous survey, without directing discussion, separate ethnographic obser-

vation readily supports some of the constructs to be used for the proposed thematic analysis. From both the independent anonymous survey and ethnographic observations during the workshops themselves, the constructs selected look well-motivated regarding cybersecurity awareness even though the underlying models (HBM, NPT) were originally conceived in a different domain.

4.3 Exploring model constructs specifically

The interviews were analysed qualitatively, using the constructs of Perceived Susceptibility, Perceived Impact and Self-efficacy from the HBM to code participant comments. Other constructs were not used systematically. Preliminary findings reveal high levels of threat awareness: participants confirmed their awareness that cyberattacks could and do occur; further, they described potential impact to their clients, and to their own products and services. This would predict an intention to engage with and deal with the cyber risks. Offering the tools demonstrated during the sessions to help understand and manage such risks would be predicted to increase Self-efficacy, not least as applied directly to each SME's own business environment as part of the demonstrations. Although they acknowledge the potential benefit of the tools in the context of cybersecurity, participants appear to avoid personal responsibility: they identified other parts of their organisation or third-party providers who should handle such matters instead.

Participants evidenced *risk awareness* associated with cyber-attacks, as predicted by the first construct of the model. They were very specific about the types of risks which could impact their business. For instance, maintaining patch levels is important not least to overcome known vulnerabilities. However, managing patch deployment would need attention:

> "… there's always a tradeoff between waiting until [a] patch has been tested in a non-production environment, and the problem that you leave the vulnerable system in the operational environment for longer" (PH)

and careful consideration of associated risks:

> "But if you apply the patch as soon as you get it, especially if you are the first in the world to do that, if you're really, really fast, then you can crash your system, right?" (PH)

The implications or *impact awareness* is also well-understood. Failure to provide access to data, would have serious consequences, for example:

> "Without this real time data, they would be like blind … being cut off completely from the market data" (PF)

as would issues with data sharing:

> “It’s mostly data protection … Always the fear that the [personal] data goes to the wrong person, either unintentionally or someone steals it” (PH)

or even in regard to tampering with software:

> “And this is very, very dangerous because somebody can hack it in a way where instead of detecting a pedestrian your model detects free space. So, this means that the car can drive on that area, which would be very, very bad” (PA)

Given this level of awareness both in terms of risk and impact, participants were positive about exploring the specific tooling being developed. They identified benefits to individual employees:

> “from [this] project, [we would like] not only a checklist but something we are able to run on… err… on a permanent way to get and to have a monitoring of all the potential security threats” (PE)

as well as for the SME as a whole:

> “but also … to the auditor. Maybe to show that that we are aware” (PF)

Participants are unsurprisingly aware that the tools being developed would be useful to support them dealing with the risks and potential impacts they had identified, therefore. But they also appreciate that to be cohesive, the tooling must handle complex perspectives and requirements:

> “We have to comply to cybersecurity threats also according to the requirements that we get from our customers … So there are quite a number of security checks that you have to comply with in order to gain the trust of the customer in order to work with them” (PA)

To be of real benefit, therefore, the visualisations the tooling offers must present a coherent view:

> “The relations are really complex, but as you just presented it, it looks relatively simple” (PF)

Participants do show, however, that their own understanding of cybersecurity issues is shifting. For example, they are beginning to think not only in terms of their own responsibilities – in this case software development – but of the overall implications for enterprise security:

> “We usually use the term safe or functional safety as opposed to security and cybersecurity” (PA)

even to the extent of prompting the demonstrators:

> “As long as you have everything … thought about everything, do not forget any assets” (PF)

showing *increased understanding* of the complexities of cybersecurity:

> “As you mentioned before … Yeah, it's … I think there are a few things you need to watch out for as well” (PF)

So, moving forward, there is a *willingness to adopt* the tooling and adapt to their own needs:

> “we would like to be able to see a potential cyberattack risk, maybe not in real time, but at least to be alerted and to react on to act” (PE)

And explore how the technology would benefit them specifically.

> “So, one of the things we're hoping to do in [the project] is model the jobs that people do and figure out if [there] are any more risk[s]” (PF)

But the prospect seems attractive:

> “…I'm absolutely excited about this and impressed” (PF)

The benefits afforded by technology in terms of *self-efficacy* were ambiguous. When shown the specific tooling being developed, there was an appreciation that tooling could benefit the individuals:

> “This this looks really, really useful for ourselves” (PF)

But the issue is more complex. Understanding regulatory requirements might not be easy in specific areas. For a non-lawyer, for example, it’s not clear that the tools might meet all the needs of individuals to extend and improve awareness:

> “Our lawyer … of course he's not [a] technical person, so he tries to translate these regulations to us but in the end I'm …I'm really not sure” (PF)

Some of the SMEs outsourced their infrastructure. This creates a dependency on a third party. And they may not provide all the information that the SME directly involved in the business might need:

> “[In] the end this I found this a little bit unsatisfying that afterwards they also did not communicate that much” (PF)

So, awareness both of potential risks and their impact may lead to a willingness to engage with tooling. However, this does not automatically relate to complete confidence in individual ability to act (*self-efficacy*). The context for SMEs is complicated by outsourcing, for example, and the range of issues which need to be considered. These are not just technical, such as monitoring and mitigating against cyber-attacks, but also regulatory in maintaining and proving compliance with industry standards and (data protection) law

With the exception of self-efficacy, therefore, the constructs from HBM and NPT are largely supported in the context of exploring operational concerns and requirements for cybersecurity tooling amongst SMEs. Given the motivation for the models used here, this would suggest that participants were aware of cyber-attack risk and impacts. On that basis, they were willing to engage with the technology since they appreciate that tooling would help address the risks identified. Further, and thinking specifically around continued adoption, support for the constructs from NPT suggest a willingness to engage further with the technology in the context of their own SME business.

5 Discussion

We interpret these preliminary results as confirmation in the first instance for the constructs of health-related models and frameworks in the context of cybersecurity technology adoption. The applicability of such models to cybersecurity and SMEs is not new [REFs]. Nor is the need to think not just about the causal behavioral model behind adoption, but the longer-term contextualization of the technology or behaviors. That being said, what we have found in this study specifically is twofold. First, that individuals need to see the utility of a given technology as it suits their own context. So, as participants describe their awareness of cyber risks and the potential benefit of the tools they were shown, they begin to engage with the technology via *cognitive participation*, as NPT formalizes it, seeing an opportunity for *collective action* to adopt and explore the tools they have been shown in their specific environment. Both the awareness indicated by the constructs of the HBM and the ongoing adoption processes from the NPT [17, 18] are necessary, of course. This confirms our previous findings [13, 14]. Their willingness to incorporate their knowledge and understanding together with the tools they were shown into the company narrative suggests the technology is being operationalized to suit their existing SME processes rather than changing their own behaviour necessarily.

Secondly, however, there is an appreciation that their operational context in regard to cybersecurity, risk assessment and mitigation is more complex than individual responsibility taking. Researchers such as Bell [REF] and Lewis and his colleagues [REF] identify cyber risks for SMEs to be resource dependent and to relate to an unwillingness to share information with potential co-competitors. The findings here suggest a different view. Individuals reported risk awareness and an appreciation of the consequences, but they also described frustration that cybersecurity involves multiple actors, whom they did not necessarily understand or who did not share all the relevant information, and factors in mitigating those risks, which prevented a level of general oversight. Self-efficacy, therefore, emerges as something beyond individual enablement. The tools demonstrated would benefit the SME as a whole, they reported, though not necessarily in their own individual job role. Risk mitigation is the responsibility of someone else after all such as an IT manager. But there was also a suggestion that they wanted to understand on an individual level what those responsible were doing and why they were doing it. Self-efficacy here does not therefore imply taking action individually but being able to appreciate the actions which are taken by others.

If, as we have suggested elsewhere, technology acceptance involves situating the technology into the company narrative, this might explain individual vulnerability [REFS 1, 4&5]. Many refuse to click on a link in a personal email received at home outside office hours, and yet, might respond to a phishing attack at work if the phishing email looks to be part of their daily tasks. So, individuals do not behave inappropriately through ignorance. Instead, they behave this way because they do not understand how their own actions fit into the overall company narrative respecting cybersecurity. Visualisation tools like those demonstrated in the workshops here need to emphasise chains of events across the socio-technical network and encourage a shared understanding of the consequences of those events.

6 Limitations and Future Work

The participants in this study were motivated to engage with the technologies being demonstrated, since all were funded through a single European project. It might be expected, therefore, that they would want to respond positively to what they were being shown and would be more attuned to identify possible benefit of those technologies. However, if - as we conclude - the discussions are consistent with other studies where even limitations in technology can be overlooked so long as what the technology offers aligns with the broader needs of the company, then other studies might provide evidence of the importance of the 'company narrative' as part of a willingness to engage with technology irrespective of any other ties between participant and researcher. Indeed, the research direction which has emerged here was not known in advance to those who took part. In the short term, we will continue to analyze this and other workshops to understand how potential adopters react to technology.

7 Conclusion

A mixed-methods approach to understand the cybersecurity imperatives for SMEs has partly confirmed findings from other studies in terms of risk and impact awareness. However, the qualitative analysis of discussion around cybersecurity visualization tools, using a coding scheme derived from well-motivated behavioral models, suggest a complex interaction between awareness, self-efficacy and situating cybersecurity into a broader company narrative. The discussions were nominally about demonstrating technology. But as SME participants engaged, they began to consider a broader narrative and not only the potential usefulness to others within their organization. Contextualizing causal behavioral models should therefore include an overall appreciation for how individuals make sense of their environment.

Acknowledgements. This work was supported by the EU H2020 CyberKIT4SME project (Grant agreement: 883188).

References

1. Sharma, K., A. Singh, and V.P. Sharma, *SMEs and Cybersecurity Threats in e-commerce.* EDPACS The EDP Audit, Control, and Security Newsletter, 2009. **39**(5-6): p. 1-49.
2. Bell, S., *Cybersecurity is not just a 'big business' issue.* Governance Directions, 2017. **69**(9): p. 536.
3. Lewis, R., et al., *Cybersecurity information sharing: a framework for information security management in UK SME supply chains.* 2014.
4. Vakakis, N., et al. *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)*. 2019.
5. van Solms, R. and J. van Niekerk, *From information security to cyber security.* Computers & Security 2013. **38**: p. 97-102.
6. Jackson, J., N. Allum, and G. Gaskell, *Perceptions of risk in cyberspace*. 2004, London School of Economics and Politics.
7. Blythe, J., *Cyber security in the workplace: Understanding and promoting behaviour change.* Proceedings of CHItaly 2013 Doctoral Consortium, 2013. **1065**: p. 92-101.
8. Ward, K., *Social networks, the 2016 US presidential election, and Kantian ethics: applying the categorical imperative to Cambridge Analytica's behavioral microtargeting.* Journal of media ethics, 2018. **33**(3): p. 133-148.
9. Martin, G., et al., *WannaCry—a year on*. 2018, British Medical Journal Publishing Group.
10. Carpenter, C.J., *A meta-analysis of the effectiveness of health belief model variables in predicting behavior.* Health communication, 2010. **25**(8): p. 661-669.
11. Champion, V.L. and C.S. Skinner, *The health belief model*, in *Health behavior and health education: Theory, research, and practice*, K. Glanz, B.K. Rimer, and B. Viswanath, Editors. 2008, Jossey-Bass: CA, USA. p. 45-65.
12. Simon, J., *Attitudes of Hungarian asthmatic and COPD patients affecting disease control: empirical research based on Health Belief Model.* Frontiers in Pharmacology, 2013. **4**(135).
13. Pickering, B., et al. *Seeing Potential is more important than usability: Revisiting technology acceptance.* in *Design, User Experience, and Usability. Practice and Case Studies. HCII 2019*. 2019. Orlando, FL: Springer, Cham.
14. Pickering, B., et al., *Ask Me No Questions: Increasing Empirical Evidence for a Qualitative Approach to Technology Acceptance*, in *Human-Computer Interaction. Design and User Experience. HCII 2020. Lecture Notes in Computer Science*, M. Kurosu, Editor. 2020, Springer.
15. Surridge, M., et al., *Modelling compliance threats and security analysis of cross-border health data exchange*, in *MEDI 2019 Workshops*, C. Attiogbé, F. Ferrarotti, and S. Maabout, Editors. 2019, Springer: Toulouse, France. p. 180-189.
16. Halvorsrud, R., Haugstveit, I. M., & Pultier, A. (2016). Evaluation of a modelling language for customer journeys. In A. Blackwell, B. Plimmer, & G. Stapleton (Eds.), Proceedings from the 2016 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC) in Cambridge, UK, 5-7. Sept 2016 (pp. 40-48). Cambridge, UK: IEEE Xplore. doi:10.1109/VLHCC.2016.7739662
17. May, C. and T. Finch, *Implementing, embedding, and integrating practices: An outline of normalization process theory.* Sociology, 2009. **43**(3): p. 535-554.
18. Pope, C., et al., *Using computer decision support systems in NHS emergency and urgent care: ethnographic study using normalisation process theory.* Bmc Health Services Research, 2013. **13**.

19. Boletsis, C., et al., *Cybersecurity for SMEs: Introducing the Human Element into Socio-Technical Cybersecurity Risk Assessment*, in *IVAPP 2021*. 2021.