I Just Want to Help: SMEs Engaging with Cybersecurity Technology *

Brian Pickering[1][0000−0002−6815−2938], Stephen C Phillips[1][0000−0002−7901−0839], and Gencer Erdogan[2][0000−0001−9407−5748]

[1] Electronics and Computer Science, IT Innovation, University of Southampton, Southampton. SO17 1BJ, UK {j.b.pickering,s.c.phillips}@soton.ac.uk
[2] Sustainable Communication Technologies, SINTEF Digital, Oslo, Norway gencer.erdogan@sintef.no

Abstract. The cybersecurity landscape is particularly challenging for SMEs. On the one hand, they must comply with regulation or face legal sanction. But on the other, they may not have the resource or expertise to ensure regulatory compliance, especially since this is not their core business. At the same time, it is also well-attested in the literature that individuals (human actors in the ecosystem) are often targeted for cyber attacks. So, SMEs must also consider their employees but also their clients as potential risks regarding cybersecurity. Finally, it is also known that SMEs working together as part of a single supply chain are reluctant to share cybersecurity status and information. Given all of these challenges, assuming SMEs recognise their responsibility for security, they may be overwhelmed in trying to meet all the associated requirements. There are tools to help support them, of course, assuming they are motivated to engage with such tooling. This paper looks at the following aspects of this overall situation. In a set of four studies, we assess private citizen understanding of cybersecurity and who they believe to be responsible. On that basis, we then consider their attitude to sharing data with service providers. Moving to SMEs, we provide a general overview of their response to the cybersecurity landscape. Finally, we ask four SMEs across different sectors how they respond to cybersecurity tooling. As well as providing an increased understanding of private citizen and SME attitudes to cybersecurity, we conclude that SMEs need not be overwhelmed by their responsibilities. On the contrary, they can take the opportunity to innovate based on their experience with cybersecurity tools.

Keywords: SME · Cybersecurity · Awareness · Training · Self-Efficacy · Innovation · Mixed Methods · Secure System Modelling

1 Introduction

Small-to-medium enterprises (SMEs) reportedly constitute 99% of businesses worldwide, employing 70% of the workforce [1]. As a sector and similar to larger,

* This work was supported by the EU H2020 project CyberKit4SME (Grant agreement: 883188).

Author accepted manuscript version of the publication by B. Pickering, S. C. Phillips & G. Erdogan.
HCI for Cybersecurity, Privacy and Trust: 5th International Conference, HCI-CPT 2023,
Held as Part of the 25th HCI International Conference, HCII 2023, Copenhagen, Denmark,
July 23–28, 2023, Proceedings. 2023, 338-352.
Published version: http://dx.doi.org/10.1007/978-3-031-35822-7_23

more resource-rich enterprises, they are subject to many regulations in addition to their day-to-day business: mandatory in the case of data protection [2] and highly desirable for cybersecurity not least for reputational reasons [3]. At the same time, SMEs suffer multiple attacks [4–7], lack resource or skill [8, 9] or budget [10, 11] to address them, and may not even have access to appropriate information to mitigate such risks [12, 13]. The risk perception literature identifies behavioural factors about cybersecurity attitudes and activities which need to be taken into account as well. Bada et al [14], for instance, highlight the need to consider perceptions and beliefs, whilst Beldad and colleagues [15] emphasise trust, and Siegrist [16] affect. Others have highlighted that overoptimism [17], lack of confidence [18, 19] (low self-efficacy [20]), of feeling personal responsibility [21], or even the attraction of doing nothing [22] may be inhibitors to risk-mitigation behaviours. Finally, Geer and his colleagues suggest that cyber risks change depending on the operational context [23]. In the empirical work presented here, we explore factors such as context, self-efficacy and responsibility from the perspective of different stakeholders in the actor network ecosystem around SMEs.

1.1 Background

The situation outlined above is exacerbated by the direct involvement of human agents for everything the SME undertakes including their employees, their clients and those they collaborate with [24, 25]. SMEs may be more vulnerable to cybersecurity threats because of their relationships with these stakeholders. For these relationships are built on mutual assumptions and dependencies: all enterprises, for example, rely on their employees to adhere to cybersecurity policy which may depend on awareness as well as willingness to conform to such policies [26]; and on their clients to respect and comply with controls [14, 27]. Figure 1 summarises some of the pressures on SMEs to engage with risk-mitigation strategies, including the main stakeholder types: human agents such as *clients* and *employees*, and institutions like *other enterprises* and *regulators*.

Notwithstanding providing advice, regulators exert an influence on SMEs to comply without the SME being able to influence behaviours of the regulator directly. With all other stakeholders, this is not the case. Employees work toward common *business objectives* to ensure the success of that SME. They are responsible, therefore, for following company policy and implementing what measures are required. At the same time, they expect the SME to provide a secure environment for them to operate and to keep any personal data about them secure. By contrast, when a client *interacts with* an SME for goods or services, they expect their data to be processed appropriately and kept secure. But at the same time, and especially in cases where a client accesses SME infrastructure such as placing an order or using a fault reporting system, the SME must equally rely on them to act in such a way as to avoid exposing the infrastructure to attack. They expect adherence to security policies, though may not have direct visibility of what clients do or of what they know. One example would be a requirement in the terms of service that the client protect their credentials or check for malware

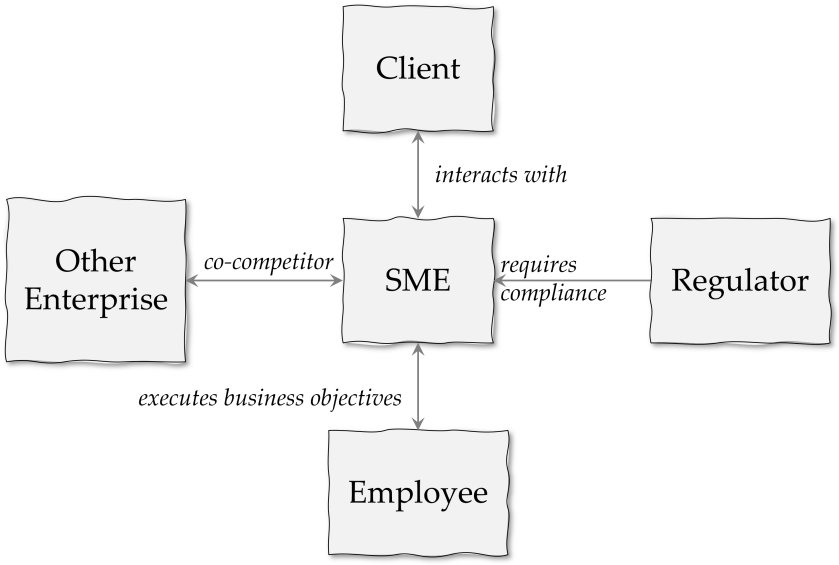

Fig. 1. Cybersecurity Landscape for SMEs

embedded in any communication they send. Finally, *other enterprises* must co-operate across a supply chain, including other SMEs, whilst at the same time exposing only limited information about cybersecurity threats and controls.

The specific purpose of this study, therefore, is to investigate cybersecurity awareness and practice amongst the stakeholders where there is a mutual expectation of security-appropriate behaviours as summarised in Figure 1.

2 Method

Against this background, we report empirical findings from three related quantitative studies exploring the attitudes and behaviours of different stakeholders in Figure 1; and a complementary qualitative study regarding SME readiness to engage with cybersecurity tooling to meet these expectations.

In addition to regulatory requirements (e.g., [2], Art 25), individuals – Clients or Employees – expect their data to be processed securely, though their own practices and lack of knowledge may be maladaptive and in turn represent a risk to the SME. Further, since an SME rarely operates alone, they must protect information exchange with Other Enterprises, and protect themselves from vulnerabilities coming from those enterprises.

Providing cybersecurity technology to support SMEs may be contextualised in technology adoption terms [28]. In this sense, the main focus has been on per-

ceived easy-to-use (PEOU) and perceived usefulness (PU). This would allow the SME to satisfy their security obligations whilst reducing their resource commitments and lack of skill (PEOU). Part of PU would include identifying the effect of the maladaptive behaviours from these groups, namely *Clients*, *Employees* but also *Other Enterprises*. Providing usable and useful technology to identify threats, knock-on effects and mitigations should be enough to guarantee tool adoption, therefore. However, our own previous work has concluded that developing a narrative around *Self-Efficacy* and motivational factors like *Innovation* may be just as significant [29].

Table 1. Summary of Participants in each Study

Study	N	Participants	Instrument	Ethics Approval
1	800	Private Citizens (UK)	Anonymous Survey	FEPS 67628 and 69107
2	470	Private Citizens (UK)	Anonymous Survey	FEPS 71408
3	141	SMEs (UK & Norway)	Anonymous Survey	FEPS 61721
4	4	SMEs (Europe)	Semi-structured Interviews	FEPS 73328

Table 1 summarises the participants in each of the four studies (numbered from 1 to 4 as in the first column of the table). Note that respondents to the anonymous surveys were principally UK based. The Private Citizens represent the *Client* type from Figure 1, whilst the SMEs represent the *Employee* as well as *Other (SME) Enterprises*. The three surveys in 2 were run via crowdsourcing platforms: *Studies 1* and *2* used *Prolific.co*, and *Study 3* used *Norstat*. Participants were self-selecting.

Table 2. Summary of Survey Instruments

Study	Description	Reference
1	Based on instrument developed and validated in [30]	Pickering & Taylor [31]
2	Derived from focus group discussions; see [32]	Pickering et al [33]
3	Derived from cybersecurity experts; see [34]	Erdogan et al [35]

Study 1 sought to identify cybersecurity awareness and competence among private individuals. Participants were balanced across gender identity, age group and ethnicity. They were randomly assigned to one of four conditions: ranking cybersecurity threats, ranking potential controls, matching threats and controls, and identifying who they believed responsible for implementing those controls. They were then asked to respond to assertions (*Strongly Agree* to *Strongly Disagree*) from a model derived from Protection Motivation Theory and previously validated by [30]. Of the 800 respondents, approximately 46% identified themselves as technology experts and 53% as comfortable with technology.

Whilst *Study 1* looked at cybersecurity attitudes, *Study 2* turned to the practical implications of such attitudes. Specifically, within the context of secure

services, how do private individuals feel about sharing their data? Again, participants were balanced across gender identity, age group and ethnicity, and were asked to respond to 48 assertions (a 6-point Likert scale from *Strongly Agree* to *Strongly Disagree*) derived from focus group discussions and divided arbitrarily into four sections. Each section began with a general question followed by 12 assertions. Each of the general questions had three choices for participants to identify when or how comfortable they felt about that particular issue. The four such questions were:

1. **Data Sharing**: who they would share their data with;
2. **Decision Making**: how they would make a data sharing decision;
3. **Privacy Concerns**: general issues around privacy;
4. **Jurisdiction**: what regulations apply.

One of each - *Data Sharing*, *Decision Making*, *Privacy Concerns*, and *Jurisdiction* - introduced each of the four groupings of 12 assertions, therefore.

Both Study 1 and 2 were contextualised in terms of health data. But whereas Study 1 explicitly asked about security threats and controls, Study 2 asked participants to consider what they expect when they share their data, that is more specifically privacy expectations. Although not wishing to conflate privacy and security, we maintain that they are related [36]. Individual behaviours around privacy and data sharing, for instance, identify the circumstances under which individuals might engage with security measures. We therefore believe Study 1 and 2 to be complementary.

Study 3 turned to SMEs themselves. Based on the results from *Studies 1* and *2*, the aim here is to understand where SMEs stand on issues of security and data handling. They may feel overwhelmed by their legal responsibilities under data protection laws, for instance, or be ill-equipped to deal with client expectations regarding responsibility. Understanding how private individual expectations map to SME capabilities would be an important finding, of course. The survey for *Study 3* consisted of 27 questions with a mixture of closed response questions allowing either single or multiple responses, and free-form text input. The questions were developed based on discussion with cybersecurity experts. They were grouped into five categories:

1. General information **about the SME** (5 questions);
2. General information **about the respondent themselves** (4 questions);
3. Information about **the ICT infrastructure** (4 questions);
4. **Cybersecurity Awareness** (8 questions); and
5. **Cybersecurity Practices** (5 questions)

Study 3 in this context is, therefore, about providing a perspective both of *Employees* and *Other Enterprises* in Figure 1.

Study 4 extends the findings of *Study 3*, focusing on *Employees* and *Other Enterprises* from a slightly different perspective. Given our previous work on SME engagement supporting the use of qualitative methods rather than just traditional technology acceptance methods [29], semi-structured interviews with

SMEs across four sectors (automotive, finance, healthcare and utilities) were conducted exploring their attitudes towards a specific modelling technology [37] to support them with their cybersecurity responsibilities in terms of other SMEs / enterprises, and with respect to individuals, be they *Clients* or *Employees*. Following previous experience, participants were simply asked to describe their attitude to cybersecurity prior to using the technology and then their experience of using the technology. Based on the three previous studies, we decided to explore indications of *Responsibility* and whether they accept such obligations; in response, whether they may feel *Overwhelmed* or alternatively believe themselves capable of meeting all demands (i.e., *Self-Efficacy*). Finally, if SMEs respond to the technology not only in terms of meeting specific needs but also in encouraging future engagement and *Innovation*. To facilitate a thematic analysis [38, 39] of the interviews, an initial coding schema was developed therefore as follows:

1. ***Responsibility***: since individuals need to feel responsible before they will engage; see [20, 21];
2. ***Overwhelmed***: to identify adaptive and maladaptive behavioural attitude; see the Extended Parallel Process Model [18, 22];
3. ***Self-efficacy***: the belief that the individual is capable of taking action; see Protection Motivation Theory [40];
4. ***Innovation***: to represent an affective aspect, having previously identified evidence that technology acceptance advantageously includes creative thinking in potential SME-based adopters [29].

Items 1, 2 and 3 relate to constructs from the Theory of Planned Behavior, of course. For instance, *Responsibility* for implementing controls derives from the construct *Normative beliefs*: what is expected by and from others. Feeling *Overwhelmed* or capable (*Self-Efficacy*) are reminiscent of the construct *Perceived Behavioral Control*: they represent the two sides of a cost-benefit analysis in deciding to act. As such, we maintain that these codes are well supported in the behavioural science literature [41]. The final code, *Innovation*, is intended to capture perceptions which go beyond the specific feeling that the SME can and should act. In the context of motivational factors [42], we believe the successful adoption of a technology should encourage feelings of autonomy, at least, an *intrinsic* motivator, which will therefore tend to be more persistent. Further, consistent with Uses and Gratifications theory [43, 44], we would expect adoption intention to be moderated by enjoyment.

3 Results

In this section, we begin by summarising the main outcomes of the quantitative studies (*Studies 1, 2* and *3*). Conclusions from these three studies then inform the interpretation of the outcomes from the final study, *Study 4*.

3.1 Study 1

Respondents ranked *If I lost my phone or laptop, or someone got my password, someone getting at my medical records* 1 or 2 (most worrying) 55% of the time; and *If the hospital gets hacked, my medical records falling into the wrong hands* 51% of the time. They were reasonably consistent, therefore, in identifying unauthorised access to data as a significant threat. Regarding controls, 71% ranked *Adding protection (encryption) to all medical data wherever it's stored, sent or viewed, so it can't be tampered with* as 1 or 2 (most effective; the next closest being *Making sure that my medical data are protected and can only be looked at by medical staff* with 40% 1 or 2 rankings). Protecting the data itself via encryption, therefore, was perceived to be the most effective control. As far as responsibility for implementing controls is concerned, overwhelmingly, participants identified the NHS or the Hospital as responsible; only in the case of *Having an automatic lock on a phone or computer app, so my data stays safe even if the phone or computer is stolen* did they see themselves as responsible.

It is clear, therefore, that private individuals *can* make decisions about threats, controls and indeed about who is responsible. In consequence, we may generalise this to say that private individuals (*Clients* in Figure 1) only see themselves responsible for implementing a control for a device they own. Otherwise, they perceive responsibility to lie with the service provider, that is the SME offering a service. In the survey [31], neither an equipment manufacturer nor service developer was regarded as responsible for the controls.

3.2 Study 2

Study 1 sought to identify a baseline of what private individual perceptions around cybersecurity might be. *Study 2* provides a complementary viewpoint: namely, is this awareness reflected in data sharing attitudes? Responding to general attitudinal questions, participants reported that they make decisions about sharing their data based on trust in the data steward (73% of the time) rather than any published privacy notice. This is important because *trust* in behavioural sciences is regarded as a willingness to expose oneself to risk [45], not reliance on rights or contract as imposed by regulation. Indeed, 84% disagree with the statement *I feel I make informed choices about privacy and data sharing.* Further, in response to the assertion *If I agree to let a company or researcher use my data, I no longer have any rights to it*, 95% agree; and for the assertion *I share responsibility for my data with whoever I release it to*, 88% disagree. whatever rights data protection affords ([2], Chapter 3) clearly do not inform decisions or empower data subjects [46].

Private individuals do not therefore necessarily understand their own rights and what these allow them to do. Data sharing decisions are based on trust in the recipient (data steward). Further, trust in that recipient seems to be influenced by what they perceive to be the likelihood of third party (onward) sharing. SME clients (see Figure 1), therefore, may not respond to assurances from the SME about how they claim to secure the data, even if they do read privacy notices

or understand their data protection rights. The expectation is that the SME assumes responsibility. This is consistent with the expectations from *Study 1*.

3.3 Study 3

Study 1 showed a reasonable level of awareness among private individuals, but an assumption that responsibility lies with the service provider. *Study 2*, primarily focused on privacy aspects of cybersecurity, reinforced the belief that service providers are responsible, but also that engagement (in this case for data sharing) is predicated on trust not regulation. With that in mind, *Study 3* looks specifically at whether SMEs report the ability to be able to provide the necessary cybersecurity context to meet private individual expectations.

Although 80% of respondents report a moderate to high degree of cybersecurity awareness, only 19% report they provide ongoing training, and 73% that they provide none. Further, 15% reported that they were aware of an attack, and 77% were not. Whether this reflects the actual situation is difficult to judge. The SMEs in question may not have been attacked (though see [47], for instance), or whether there is no internal communication of security incidents. Finally, only 16% reported that they use specific tools to identify and mitigate against cyber attacks; 62% do not, and 23% reported they didn't know. Overall, and despite reporting a reasonable level of understanding, there is a lack of training and tool implementation to mitigate against cyber threats should they occur.

In *Study 1*, it was clear that clients almost always expect a service provider to assure the security of their data, and *Study 2* that they believe themselves at the mercy of service providers, having no control once they have shared their data. The onus therefore is perceived to be on SMEs to protect data, but this third study highlights that they are not necessarily in a position to assume this responsibility. More importantly, though, is that if engagement with the SME is based on *trust* as suggested by *Study 2* rather than policy or regulation and shared responsibility, then there is a significant reputational risk to the SME. In the context of the SME collaborating with Other Enterprises, although the assumption is that working together will be subject to compliance with a service-level agreement, non-disclosure agreements, or other contractual instruments - rather than trust - this reputational risk needs to be addressed.

3.4 Study 4

The first two studies indicate that responsibility for security and associated privacy rests with the SME. The third highlights a concern that training and tools are not used sufficiently, and therefore the SME may not be in a position to assume such responsibility. In the fourth and final study, we engaged directly with SMEs whose business was largely dependent on maintaining the trust of their end-user clients and the security of their data. For the interviews, we asked the SMEs to describe their experience with a specific security modelling tool. As outlined above, a coding scheme was used to identify relevant themes from

the interviews. (Note that the SMEs are referred to as P1 to P4; there were two employees involved for P1 and P4, and one for P2 and P3).

Starting with *Responsibility*, the SME interviewees report an awareness that they are responsible for the data from their clients, but also to support their non-technical staff members in appreciating the importance of security:

> (P2)... we collect some sensitive data ... we should protect them and also, [control] access to... to our servers ... and also [help] understand that our nontechnical employees how to protect them [*sic.*] data and so... so our customers data

They recognise, therefore, and accept that they are responsible for their infrastructure (*our servers*), the data they process (*we should protect them*), and have an obligation to train or raise awareness with their own staff (*[help]... our nontechnical employees to protect ... data).*

> (P4) Sometimes there are some sensitive data and sensitive projects and they just want it [*sic.*] to be 100% sure that everything is secured from our side. So we should spend a lot of money on this.

They appreciate, though, that such obligations demand resource, in this case, financial. Notwithstanding the financial implications, in attempting to meet these obligations, they can become *overwhelmed*. Without training and tooling (see *Study 3*), it may not be possible to move beyond this state:

> (P4) We didn't know how to handle [an] attack from the outside if something is... not safe in our office.

further:

> (P1) it's complex and the models are getting huge and complex really quickly

and

> (P2) Maybe it's a bit difficult to manage all threats that we found because sometimes there are a lot of all of them

Feelings of being *overwhelmed* mean that the SME may fail to provide the level of service security that their clients and enterprise partners expect. However - and remembering that the SMEs were simply asked to describe their experience as opposed to respond to specific questions on the security tool – the SMEs also report an increase in *Self-Efficacy*:

> (P1) we have to model the overall architecture of the infrastructure and [with this tool] we can see where are the caveats of this infrastructure ... where we need to intervene

and

> (P2) I think in the future we can understand how... how to apply..., for example, these are risk reports

If they use appropriate tools, therefore, the SMEs in *Study 3* who do not use tools are missing out, especially given that clients expect them to be responsible, and despite a possible lack of resource as reported in the literature, would nevertheless be in a better position to meet the expectations of their clients with appropriate tooling.

Beyond that, with increasing familiarity with such tooling, the SMEs interviewed began to identify other uses that they were not necessarily aware of originally. Although task-orientated, there is nevertheless a sense that it's not just about utility (PU), but also a sense that they are looking for other opportunities to use the tools, and to extend their own understanding:

> (P1) What can come out of the model that we we create ... the [threat] path ... that we can see once we finish the model and we sort out all the threats and we can see the threat paths where an attacker might steal information or we have information leak. But for us, I think it will be *great advantage*."

(our emphasis), and:

> (P3) there is [the] GDPR compliance issue and possible modelling errors. So, this part of the tool it's very... important and interesting

What emerges from our interviews is that the SMEs in *Study 4* are aware of their responsibilities and can feel over-faced: cybersecurity is too complex and beyond their core competence. However, with suitable tooling (which is often missing, as in *Study 3*), the SME is not only able to meet their commitments (their *Self-efficacy* increases), but they begin to see other and more generalised potential with the tooling (*Innovation*). We suggest that this actually influences cybersecurity technology acceptance, which complements its importance for risk perception and adaptive behaviours in individuals [48–50].

Close collaboration from tool vendors with the SMEs, including encouraging them to explore the potential of cybersecurity tools rather than simply check that the tools meet *a priori* requirements, means that they are able to fulfil the expectations of their clients as well as comply with regulation. Such narratives take them beyond feeling overwhelmed to self-efficacy and the development of innovation [29]. And this is in parallel with their basic business, even though SMEs are generally assumed to lack (and report, see (P4)'s comments above on money implications) the resource to support anything beyond their core business.

4 Discussion

The four studies reported here had been run independently. There had been no overall plan to develop a coherent research approach to identify the challenges for

the SME security landscape and expectations of their stakeholders. It is perhaps all the more remarkable that there is an emerging narrative from SMEs who engage with cybersecurity tooling that they not only meet their obligations but can also start to see ahead for other opportunities for security technologies to support their business and reputation. Despite confused client expectations, for instance, their lack of understanding of their rights under data protection and the abdication of responsibility to others when sharing their data, even just thinking about appropriate tools can expand SME self-efficacy and their ability to meet their obligations while maintaining their reputation vis-à-vis their stakeholders.

Our findings are not inconsistent with what has already been documented regarding private individuals. It is well-attested, for instance, that regulation does not necessarily empower private individuals [46]: they feel overwhelmed. In that context, it is no surprise in *Study 2* to discover that private individuals do not believe themselves to retain control over their data, even though they may be aware of cyber threats and suitable controls to mitigate them (*Study 1*). Further, even though regulation imposes responsibilities on those who process personal data [2], if SMEs are not completely aware of the threats they are exposed to, do not provide the training, and do not exploit predictive or preventative tooling (*Study 3*), there is a serious risk to multiple players, not least given the pervasiveness of SMEs [1]. What we have found in bringing the results from these studies together is that engagement with tooling can encourage *Self-efficacy* but also *Innovation* within the SME.

The project developing the security tools focused on close collaboration and support for the SMEs who took part in *Study 4*. Significantly, though, the interviews reported here were not about checking that requirements had been met with the tools in questions. Instead, they were given free rein to describe whatever their experience had been. Their response, as reported above, in developing the appropriate *Self-Efficacy* to meet their responsibilities has led them to think creatively (*Innovation*): seeing additional potential in the tools [29], without reporting any concerns about the resource implications of engaging with them. This seems to meet a significant need. Whatever the data subject rights are that regulation foresees, private individuals do not appear to be reassured and still believe their data are at the mercy of service providers. This imposes an obligation on the SMEs, though, which is more about reputation and the ongoing negotiation around mutual trust. To enable SMEs to go beyond their statutory regulatory obligations and focus on the trust of their clients, they need to be supported to understand how tools work with and for them, not simply tick a box: *Study 3*, for example, highlights that awareness does not necessarily translate into action. The aim of tool vendors shifts therefore away from compliance towards enabling the SMEs to feel empowered to handle cyber security.

Study 4 shows that a disparate set of SMEs across finance, healthcare, automotive and utilities can be helped along this path. So, even though private individuals do not understand their rights or responsibilities, SMEs can nonetheless develop and maintain their trust.

5 Limitations and Future Directions

The studies reported here were not part of a coherent research plan, as stated above. Further, the SMEs in *Study 4* were collaborators on a common project. It is not clear, therefore, how representative they are of the SME cohort in *Study 3*. The connection between the first three studies and the final one may not be self-evident, therefore. That being said, that a narrative is developing of how SMEs can meet the expectations beyond what they are required to do suggests that in future a coordinated set of studies focused on the various aspects covered here may identify what support needs to be delivered to SMEs above and beyond generic awareness and training programmes. In so doing, a set of concrete recommendations can be generated to encourage SMEs faced with their responsibilities regarding security to engage with cybersecurity tools not just from ensuring preparedness for possible cyber attacks but also as a starting point to think innovatively about how they use tools in-house. Intrinsic motivation is known to be more robust than short-term extrinsic motivators like rewards and sanctions [42]. Encouraging a sense of self-fulfilment which seems to lead to innovation may encourage employees to assume responsibility for security compliance rather than imposing it on them. This would need further investigation.

6 Conclusion

Our research has examined different aspects of the SME cybersecurity landscape from different, stakeholder perspectives, and highlights different expectations and actual behaviours. Whatever regulation is in place which imposes obligations on SMEs, such regulation does not necessarily correspond with the expectations of private individuals. Further, SMEs themselves may be ill-equipped to meet their regulatory obligations but also to address customer expectation. Exploring how they use and could use cybersecurity tools can encourage self-efficacy, and therefore enable the SME to satisfy both. The interviews conducted here – based just on a generalised description of benefit to the individual – provides further evidence for introducing qualitative methods into our understanding of technology adoption.

7 Ethics

The various studies reported here were provided separate approval from the Faculty of Engineering and Physical Sciences (FEPS) Research Ethics Committee at the University of Science. The reference numbers are shown in the final column of Table 1 above.

References

1. Lin, D.-Y., Rayavarapu, S.N., Tadjeddine, K., Yeoh, R. : Beyond financials: Helping small and medium-sized enterprizes thrive. In: McKinsey & Company, Public

& Social Sector Practice, 2022, https://www.mckinsey.com/industries/public-and-social-sector/our-insights/beyond-financials-helping-small-and-medium-size-enterprises-thrive
2. European Commission: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (2016)
3. International Organization for Standardization: ISO/IEC 27000:2018, in Information technology — Security techniques — Information security management systems — Overview and vocabulary. 2018
4. Wilson, M., McDonald, S., Button, D., McGarry, K.: It Won't Happen to Me: Surveying SME Attitudes to Cyber-security. Journal of Computer Information Systems. 1–13 (2022) https://doi.org/10.1080/08874417.2022.2067791
5. Khan, M.I., Tanwar, S., Rana, A.: The Need for Information Security Management for SMEs. In: 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)., pp. 328–332. IEEE, Moradabad, India (2020)
6. Bell, S.: Cybersecurity is not just a 'big business' issue. Governance Directions. **69**(9), 536–539 (2017)
7. Sharma, K., Singh, A., Sharma, V.P.: SMEs and Cybersecurity Threats in e-commerce. EDPACS The EDP Audit, Control, and Security Newsletter **39**(5–6), 1–49 (2009)
8. Blythe, J.: Cyber security in the workplace: Understanding and promoting behaviour change. In: Bottoni, P., Matera, M. (eds.) Proceedings of CHItaly 2013 Doctoral Consortium, 1065, pp. 92–101. Trento, Italy (2013)
9. 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), pp. 1–5. IEEE, Dublin, Ireland (2020)
10. 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, ACM, Cambridge, UK (2017) https://doi.org/10.1145/3102304.3109812
11. Blythe, J.M., Coventry. L.: Costly but effective: Comparing the factors that influence employee antimalware behaviours. Computers in Human Behavior **87**, 87–97 (2018)
12. Gafni, R., Pavel, T.: The invisible hole of information on SMB's cybersecurity. Online Journal of Applied Knowledge Management (OJAKM) **7**(1), 4–26. (2019)
13. Wachinger, G., Renn., O., Begg, C., Kuhlicke, C. : The Risk Perception Paradox - Implications for Governance and Communication of Natural Hazards. Risk analysis **33**(6), 1049–1065. (2013) https://doi.org/10.1111/j.1539-6924.2012.01942.x
14. Bada, M., Sasse, M.A., Nurse, J.R. : Cyber Security Awareness Campaigns: Why do they fail to change behaviour? In International Conference on Cyber Security for Sustainable Society. pp. 118-131. Coventry, UK. (2015)
15. Beldad, A., de Jong, M., Steehouder., M.: How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. Computers in Human Behavior **26**(5), 857–869 (2010) https://doi.org/10.1016/j.chb.2010.03.013
16. Siegrist, M.: Trust and Risk Perception: A Critical Review of the Literature. Risk Analysis. **41**(3), 480–490. (2021) https://doi.org/10.1111/risa.13325
17. De Kimpe, L., Walrave, M., Verdegem, P., Ponnet, K.: What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. Behaviour& Information Technology. **41**(8), 1796–1808. (2022). https://doi.org/10.1080/0144929X.2021.1905066

18. Witte, K.: Putting the Fear back into Fear Appeals: The Extended Parallel Process Model. Communication Monographs. **59**(4), 329–349 (1992).
19. Witte, K., Allen, M.: A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns. Health education & behavior. **27**(5), 591–615 (2000). https://doi.org/10.1177/109019810002700506
20. Rimal, R.N., Real, K.: Perceived Risk and Efficacy Beliefs as Motivators of Change. Human Communication Research. **29**(3), 370–399. (2003)
21. Paek, H.-J., Hove, T.: Risk Perceptions and Risk Characteristics. In: Oxford Research Encyclopedia of Communication. Oxford University Press (2017)
22. Bax, S., McGill, T., Hobbs, V.: Maladaptive behaviour in response to email phishing threats: The roles of rewards and response costs. Computers & Security. **106**, 102278 (2021) https://doi.org/10.1016/j.cose.2021.102278
23. Geer, D., Jardine, E., Leverett, E.: On market concentration and cybersecurity risk. Journal of Cyber Policy. **5**(1), 9–29 (2020) https://doi.org/10.1080/23738871.2020.1728355
24. Öğütçü, G., Testik, Ö.M., Chouseiniglo, O. : Analysis of personal information security behavior and awareness. Computers& Security. **56**, 83–93, (2016) https://doi.org/10.1016/j.cose.2015.10.002
25. Lewis, R., Louvieris, P., Abbott, P., Clewley, N., Jones, K.: Cybersecurity information sharing: a framework for information security management in UK SME supply chains. In: Twenty Second European Conference on Information Systems, Tel Aviv, Israel (2014)
26. D'Arcy, J., Hovav, A., Galletta, D.F.: User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach, Information Systems Research, **20**(1), 79–98 (2009) https://doi.org/10.1287/isre.1070.0160
27. Morrow, B.: BYOD security challenges: control and protect your most sensitive data. Network Security. **2012**(12), 5–8 (2012) https://doi.org/10.1016/S1353-4858(12)70111-3
28. Davis, F.D.: Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS quarterly. **13**(3), 319–340 (1989) https://doi.org/10.2307/249008
29. Pickering, B., Phillips, S., Surridge, M.: Tell me what that means to you Small-story narratives in technology adoption. In: HCI INTERNATIONAL 2022. Springer Nature, Gothenburg, Sweden (2022) https://doi.org/10.1007/978-3-031-05311-5_19
30. Ifinedo, P.: Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computer & Security. **31**(1), 83–95 (2012) https://doi.org/10.1016/j.cose.2011.10.007
31. Pickering, B., Taylor, S.: Cybersecurity Survey. https://zenodo.org/record/7589508
32. Boniface, M., Carmichael, L., Hall, W., McMahon, J., Pickering, B., Surridge, M., Taylor, S., Baker, K., Atmaca, U. I., Epiphaniou, G., Maple, C., Murakonda, S., Weller, S.: DARE UK PRiAM Project D4 Report: Public Engagement: Understanding private individuals' perspectives on privacy and privacy risk. https://zenodo.org/record/7107487
33. Pickering, B., Baker, K., Boniface, M., McMahon, J.: Privacy Perspectives Survey. https://zenodo.org/record/7589522
34. Erdogan, G., Halvorsrud, R., Boletsis, C., Tverdal, S., Pickering, J.B.: Cybersecurity Awareness and Capacities of SMEs. In: 9th International Conference on Information Systems Security and Privacy. Lisbon Portugal (2023)

35. Erdogan, G., Halvorsrud, R., Boletsis, C., Tverdal, S., Pickering, J.B.: Cybersecurity Awareness and Capacities of SMEs. International Conference on Information Systems Security and Privacy (ICISSP), Lisbon, Portugal. (2022) https://doi.org/10.5281/zenodo.7443048
36. Edelman, S., Peer, E.: Predicting privacy and security attitudes. ACM SIGCAS Computers and Society. **45**(1), 22–28 (2015) https://doi.org/10.1145/2738210.2738215
37. Chakravarthy, A., Chen, X., Nasser, B., Surridge, M.: Trustworthy systems design using semantic risk modelling. In: 1st International Conference on Cyber Security for Sustainable Society, Coventry, UK (2015)
38. Braun, V., Clarke, V.: Using thematic analysis in psychology. Qualitative research in psychology. **3**(2), 77–101 (2006) https://doi.org/10.1191/1478088706qp063oa
39. Braun, V., Clarke, V.: Reflecting on reflexive thematic analysis. Qualitative Research in sport, exercise and health. **11**(4), 589–597 (2019) https://doi.org/10.1080/2159676X.2019.1628806
40. Chenoweth, T., Minch, R., Gattiker, T.: Application of Protection Motivation Theory to Adoption of Protective Technologies. In: 42nd Hawaii International Conference of System Sciences. IEEE, Waikoloa, HI, USA (2009)
41. Ajzen, I: The theory of planned behaviour: Reactions and reflections. Psychology & Health **26**(9), 1113–1127 (2011) https://doi.org/10.1080/08870446.2011.613995
42. Deci, E.L., Ryan, R.M.: The "what" and "why" of goal pursuits: Human needs and the self-determination of behavior. Psychological inquiry. **11**(4), 227–268 (2000) https://doi.org/10.1207/S15327965PLI1104_01
43. Ruggiero, T.E.: Uses and Gratifications Theory in the 21st Century. Mass Communication & Society. **3**(1), 3–37 (2000) https://doi.org/10.1207/S15327825MCS0301_02
44. Camilleri, M.A, Falzon, L.: Understanding motivations to use online streaming services: integrating the technology acceptance model (TAM) and the uses and gratifications theory (UGT). Spanish Journal of Marketing - ESIC. **25**(2), 217–238 (2021) https://doi.org/10.1108/SJME-04-2020-0074
45. Mayer, R. C., Davis, J. H., Schoorman, F. D.: An Integrative Model of Organizational Trust. The Academy of Management Review. **20**(3), 709–734 (1995) https://doi.org/10.5465/AMR.1995.9508080335
46. Acquisti, A., Brandimarte, L., Loewenstein, G.: Privacy and human behavior in the age of information. Science **347**(6221), 509–514 (2015) https://doi.org/10.1126/science.aaa1465
47. Jahankhani, H., Meda, L.N.K., Samadi, M.: Cybersecurity Challenges in Small and Medium Enterprise (SMEs). In: Jahankhani, H., V. Kilpin, D., Kendzierskyj, S. (eds) Blockchain and Other Emerging Technologies for Digital Business Strategies. In Advanced Sciences and Technologies for Security Applications. Springer, Cham. (2022) https://doi.org/10.1007/978-3-030-98225-6 1
48. Slovic, P., Peters,E.: Risk perception and affect. Current directions in psychological science. **15**(6), 322–325 (2006)
49. Van Schaik, P., Renaud, K., Wilson, C., Jansen, J., Onibokun, J.: Risk as affect: The affect heuristic in cybersecurity. Computers & Security. **90**, 101651 (2020) https://doi.org/10.1016/j.cose.2019.1016510167-4048/
50. Slovic, P., Finucane, M.L., Peters, E., MacGregor, D.G.: Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality. Risk analysis. **24**(2), 311–322 (2004) https://doi.org/10.1111/j.0272-4332.2004.00433.x