Risk and the Small-Scale Cyber Security Decision Making Dialogue — a UK Case Study

Emma Osborn and Andrew Simpson

Department of Computer Science, University of Oxford, Oxford OX1 3QD
Email: Emma.Osborn@cybersecurity.ox.ac.uk; Andrew.Simpson@cs.ox.ac.uk

Despite a long-standing understanding that developments in personal and cloud computing practices would change the way we approach security, small-scale IT users (SSITUs) remain ill-served by existing cyber security practices. This paper discusses results from a survey that considered (in part) cyber security decisions made by SSITUs. We determine that: SSITUs are focusing on easy-to-implement technical measures, leading to a disconnect between the security implemented and any risks identified; available resources, knowledge, prioritisation of business processes, reduced system control and a lack of threat intelligence all combine to limit the ability to make cyber security decisions; and assessing risk in SSITUs will not lead to sufficient investment to mitigate risks for risk-holding stakeholders in the supply chain. We conclude that the constraints faced by SSITUs have far greater impact on the decisions they make than either our risk-holding, or security-providing, participants may have anticipated. Any limitations faced by SSITUs as they make their security decisions will have a significant impact on both the measures they are able to apply and the security of the supply chain as a whole.

Keywords: Cyber Security; Risk Management; Decision Making; SME; Charity; Home Users; Supply Chain

Received 00 January 2009; revised 00 Month 2009

1. INTRODUCTION

Technology is used pervasively by individuals, families and small organisations. With internet penetration growing yearly in almost every country, developed countries now typically have over 80% of their populations online[1] and in the UK small companies (defined as employing fewer than 50 people) account for 99.3% of all private sector businesses and 48% of employment[2]. Despite this, neither individuals nor small organisations typically spring to mind when one considers the term *cyber security*.

The impact of the widespread adoption of ICT by small organisations on cyber security is by no means a new phenomenon. Two decades ago Carroll [1] wrote:

> "Today the PC is the computing platform of choice for most small and medium-sized businesses ...
>
> ... Most books on security were written for big-time users like banks and government agencies where enormous sums of money, or state secrets were at stake. Most PC systems could never meet the security requirements of these mainframe and minicomputer systems. And if they could, the average business or professional person could neither afford them nor be bothered maintaining them." [1]

As early as 1996, with the rapid growth of personal computing, people were differentiating the actions and requirements of small-scale IT users (SSITUs — defined in Section 2) from those of large organisations, highlighting the infrastructure, threat landscape, resource and relative importance of issues pertaining to security for smaller organisations.

Despite the problem being long highlighted, as well as by authors recognising the impact of moving to a more distributed computing model, the question of the different security requirements faced by SSITUs has, unfortunately, been left largely unresolved.

Pfleeger and Pfleeger highlight how the ubiquity of computing has given users a responsibility for security that they have neither the awareness nor the motivation to handle — leading to a mismatch between security

[1]The World Bank Internet users (per 100 people in 2015): `data.worldbank.org`

[2]`www.gov.uk/government/statistics/business-population-estimates-2015`

measures and risks [2]. This pattern is repeated in the UK's 2016 National Cyber Security strategy report, which stated that smaller businesses' *"awareness of the personal relevance of the cyber risk is patchy"*[3].

We report results of an empirical study that evaluated SSITU technology use, with respect to their ability to justify security investment, within a broader ecosystem of small-scale cyber security stakeholders in the UK. The survey was motivated by a lack of available data about the environment in which these small organisations make their cyber security decisions, which makes designing security measures specific to the sector challenging. Notably, we document what SSITUs *are doing* to counterbalance arguments that they are failing to implement cyber security best practices.

A previous study highlighted how *security* experts' assumptions that common security practices are scalable to small organisations acted as a barrier to entry for *small business* experts/owners [3]. Experts' experiential knowledge from working in larger organisations, combined with a lack of SME engagement with research, may be as influential on small-scale cyber security as the decisions made by small organisations.

In this paper we focus on decision making and risk assessment (RA) practices within SSITUs, comparing the processes implemented with common corporate cyber security practices. The identification of risks is the cornerstone of justifying cyber security expenditure, irrespective of the size or mission of an organisation. With SSITUs often looking inwards to evaluate cyber risk and institute appropriate security measures, it is understandable that our participants reported that understanding risk management requirements and cyber threats was the most difficult aspect with regards to cyber security. But, as RA and management processes play such a key role in cyber security good practice, we wish to ask *how do the constraints of a small organisation influence their risk perception and how they justify security investment?*

With a view to answering this question, we have explored a number of decision-making concepts discussed by our survey participants. Section 2 describes the methodology used in the survey. We then discuss how (irrespective of risks or their mitigations) the context within which SSITUs operate alters their decision-making priorities. In Section 4 we use a scenario, based on descriptions from our participants, to evaluate the different stages of a lightweight risk assessment process, describing the difficulties an SME might have in using security best practices to identify their risks. Section 5 explores how a better understanding of risk, alongside some other considerations highlighted by our participants, could incentivise SSITUs to improve their security.

In addition to the constraints on knowledge and resources faced by SSITUs, there is also the issue of operating with increasingly distributed systems, with the associated issues of complexities in system control and ownership. Systems are becoming inextricably linked, changing the cyber security risk landscape and introducing issues of influence into the discussion of SSITUs' ability to treat risk. As such, Section 6 discusses incentives for risk-holding stakeholders to secure the supply chain. We draw our conclusions and consider possible areas of future work in Section 7.

2. METHODOLOGY

This paper discusses some initial results relating to the identification of cyber security risk by SSITUs in the UK, which have emerged during our broader study into their cyber security requirements [4].

The aim of this research is to understand the security needs of SSITUs, how that is reflected (or otherwise) in current security practices, and what impact this may eventually have on the supply chain. To this end, an initial study [3] aimed to gather information about cyber security practices in SMEs. Although providing useful data (described in Section 2.2), the initial study also faced the issue of SME owners' and directors' lack of interest in engaging with cyber security research.

Attempts at random sampling through mailing lists, etc. resulted in a response rate of less than 1%. The majority of responses originated from advertising the study on social media or making direct requests to business acquaintances. For this reason the ability to collect data and its format played a central role in determining the project design — it would not, for example, be possible to carry out a large-scale quantitative study of the ways in which small businesses use technology.

As such, we take a *qualitative* approach, similar to that employed by [5] and [6], employing a meta-study of the sector, which combines the results of our empirical study with recent results from different fields of research and views of stakeholder groups.

2.1. Scoping and defining stakeholders

We identify three (not mutually exclusive) stakeholder groups in the small-scale cyber security ecosystem:

1. small-scale IT users (SSITUs);
2. those providing cyber security measures to this user group (SP); and
3. those concerned about the implementation of cyber security by SSITUs (typically risk-holders (RH)).

SSITUs are the entities without sufficient resources, infrastructure or requirements to warrant deploying the (often expensive) corporate cyber security model. This includes small to medium-sized enterprises (SMEs — using the European Commission's definition[4]), startup

[3] www.gov.uk/government/publications/the-uk-cyber-security-strategy-2011-2016-annual-report

[4] What is an SME? European Commission 2014: ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/

Data Source	SSITU	SP	RH	TS
Questionnaire	33 SMEs			≈60% L
Interview 1	•			H
Interview 2		•	•	H
Interview 3	•			H
Interview 4	•			L
Interview 5	•	•		L
Interview 6	•	•		L
Interview 7		•		L
Interview 8	•	•		H
Interview 9		•	•	L
Interview 10		•		H
Interview 11			•	H
Interview 12		•		L
Interview 13		•	•	L
Interview 14	•			H
Interview 15		•		H
Interview 16	•			H
Interview 17	•			L
Interview 18			•	H
Interview 19	•	•		H
Interview 20		•		L

TABLE 1. Dataset overview

companies, volunteer-run organisations such as small charities or private clubs, families and individuals.

The other stakeholders for small-scale cyber security have influence on the decision-making dialogue, often without being small organisations themselves. This is typically either by imposing security expectations or requirements on SSITUs, or by influencing their access to security information or products.

2.2. Data collection and analysis

We use two primary data sources, the first of which was a questionnaire aimed at small to medium-sized enterprises (SME) owners, directors and managers, which provided an initial dataset. There were 33 respondents to the initial questionnaire, from 19 different industry sectors. The sector with the highest number of respondents was IT and telecoms (8), and there were 11 respondents who provided professional services other than IT. Respondents were distributed across 15 UK counties, with one response from a company outside of the UK. There were 8 respondents in single person companies, 13 in micro companies of more than one person, 10 in small companies, and 2 in medium-sized companies[5].

The initial dataset was used to guide sampling in the collection of a more substantial qualitative dataset, increasing the level of detail about the technology employed by SMEs and encompassed those small-scale cyber security stakeholders excluded by the SME definition. This second phase of data collection consisted of 20 detailed unstructured interviews with a variety of participants spanning all three of the stakeholder groups described in Section 2.1 — an overview of our dataset can be found in Table 1. In some interviews (8 of 20) participants talked about multiple organisations — as directors of multiple companies, comparing work and home decisions, describing customer practices, or providing real-life context to the description of reported crimes. For context Table 1 also provides information on the technical skills (TS — low (L) or high (H) — based on whether the participant reported having a technical background) each participant had when making decisions about cyber security.

Where applicable, we also make use of secondary data sources, such as the description of data breaches in Monetary Penalty Notices issued by the UK Information Commissioner's Office[6].

Due to our qualitative approach sampling was *theoretical*, rather than random [7]. We followed the recommendation of Guest et al. [8] to conduct 12–20 interviews, and participants were recruited to assist in our identification of the themes that help to describe the small-scale cyber security ecosystem — with the aim being to develop a breadth of understanding.

The insights we share throughout this paper are the result of a Grounded Theory analysis of our dataset. Corbin and Strauss describe it as a methodology that facilitates *"building theory from data"* [9]: it does not begin with a theory in mind; rather, it begins with an area of study (in this case the use of cyber security in small organisations) and allows a theory to emerge from the data. This research method is particularly suited to providing insight into real-world issues where little is known from the perspectives of certain stakeholders, making it ideal for our purpose. Where applicable, we provide an example from the raw data to assist the reader's understanding of a theme under discussion.

3. THE CONTEXT OF SSITU CYBER SECURITY DECISION MAKING

In the following, we use empirical accounts of interviewees' processes to begin evaluating security practices in the small-scale cyber security ecosystem. As with any business decision, SSITU decision makers will have to balance investments in cyber security with other competing factors.

In order to understand SSITUs' approaches to cyber security, we must first understand the environment in which these small organisations operate. The following subsections outline some of the main constraints faced by SSITUs, grouped into three concepts that emerged from our dataset: the prioritisation of business decisions; limited resources; and a knowledge vacuum.

sme-definition/indexen.htm

[5]The results of this initial feasibility study can be found in [3] with a detailed description of the methodology in an extended technical report: http://ora.ox.ac.uk/objects/uuid:4363144b-5667-4fdd-8cd3-b8e35436107e

[6]ico.org.uk/action-weve-taken

3.1. Business decision making

As we saw in Section 2, not all SSITUs are businesses. However, when making decisions about cyber security, all SSITUs will weigh the reduction of risk against their need to use technology to facilitate another process. For example, one participant explained how, when travelling, he used mobile networks to connect to the internet to make his own internet use more secure. Once he had consumed his contracted data allowance he would then switch to the Wi-Fi supplied by the bus or train companies, thereby valuing continuous connectivity above increased security. SSITUs in our study could be seen to be prioritising availability over confidentiality in their security decisions.

In their definition of small enterprises Wynarczyk et al. [10] highlight *uncertainty* — such entities are 'price-takers', vulnerable due to a high dependence on external influences and far too small to affect market values. This means that small organisations operate with higher risks than larger companies do, and, as such, may not consider cyber security risk as being more significant than the other potentially catastrophic risks that they face. All decision makers have to balance the security decisions they make with other activities that need investment [2]; however, the combination of resource constraint and lack of influence increases contention in decisions made by this group.

3.1.1. Protecting business processes

Many reasons were given by our participants for prioritising business processes over increased security. These include:

- maintaining service levels and consequently customer goodwill;
- a reluctance to update incumbent processes;
- process avoidance or immaturity in startups;
- flexibility in device use, especially during travel; and
- a lack of sufficient IT infrastructure in which to adopt good practice.

In some cases our participants indicated a reluctance to improve security due to the level of reliance on a legacy process and the level of disruption and risk that would result from changing this process. Lee and Xia [11] support this view, describing how — due to resource constraints — SMEs have less redundancy, making them less able to test a variety of solutions before making the decision to switch.

Our data shows a difference in the receptivity of different types of organisation to security processes: sectors that are naturally risk-averse (e.g. accountancy) or compliance-heavy (e.g. manufacturing) tend to be more receptive of security standards.

The study highlighted how clubs and societies had volunteers with specialist interests making decisions about certain processes. The prioritisation of decisions in voluntary organisations therefore depends on the demographics of the committee, although, in the case of charities, some financial justification of decisions has to be reported. One participant mentioned that committee members have to begin their roles "switched on", as these small, committee-led organisations can lack leadership stability, not giving volunteers the time to learn a new role and often leading to knowledge leaving the organisation without notice.

One risk that a participant highlighted (in conjunction with a lack of knowledge) is the risk of indiscriminate security — blind mitigation following product fashions and prescriptive guidelines could damage undocumented socio-technical processes. This highlights why SMEs in particular were slower to adopt advice — evidence that the benefits of risk reduction need to outweigh the risks of disrupting undocumented processes that have no redundancy.

3.1.2. System complexity

Complexity also has a role to play in decision making. In large organisations the decision makers have responsibility for both higher budgets and risks — the complexity is proportionate to the organisation but the decision makers are usually specialised in the area they have responsibility for [12].

In comparison, SSITUs have a different set of problems. Each decision maker directing the organisation might hold multiple roles, making them less specialised in the subjects they are making decisions about. More importantly the majority of our participants described how multiple organisations (through the different work, volunteer and private roles a SSITU plays) all shared the same IT resources, giving rise to a potential conflict of interest for the decision maker. Should, for example, a business owner operating from home influence the whole family's internet use?

Security measures often restrict access, so decisions made for one role could have a significant impact on the decision maker's ability to function in their other roles. Understanding where this conflict of interest may exist is particularly important to any RH stakeholder entering into an agreement with a SSITU.

3.2. Resource constraint

Resource constraint (both human and financial) was highlighted by our participants as a major factor in the allocation of security budgets.

3.2.1. Human resources

SSITUs have a limited number of employees, but still need to carry out activities similar to those carried out by large organisations. The difference is a lack of specialisation [12]: participants in our study indicated that companies had to reach a critical mass of around 25 employees before an IT function was defined.

The dependencies that small organisations have on

external factors, highlighted by Wynarczyk et al. [10], force them to limit the size of their workforce to improve their resilience to changes in uncontrollable costs; this helps explain why a number of participants suggested that a lack of engagement with security is a result of SMEs being "busy running their companies". Processes linked to revenue generation and customer satisfaction are prioritised over maintenance processes during all but the quietest periods.

The impact of having a lack of *knowledgeable* IT staff is discussed in Section 3.3.

3.2.2. Cyber security budgets

Some of the issues discussed in this section are inherent to small organisations; however, small organisations are clearly doing a cost-benefit analysis in implementing their security measures, in line with good practice [2]. A small cyber security budget alone does not necessarily translate to poor cyber security practice and one issue in the small-scale cyber security dialogue is a lack of SMEs managing the expectations of the larger organisations in their supply chains.

Quantified budgets from the questionnaire dataset, combined with discussion in subsequent interviews, highlighted 3 factors RH and SP stakeholders may wish to be aware of:

1. Two separate business cases emerged, differentiating between financing cyber security as a business process and financing a saleable capability or professional reputation.
2. As would be expected, the budget a company is willing to allocate on cyber security increases with the size of the company, making it possible to estimate a cyber security budget as a per-person value. Micro- and small companies invested £10-50 per person per year where cyber security was just another process. Small companies (10-49 people) where cyber security was a capability were investing £110-500 per person per year, which is likely to be the cost of transitioning from home security practices to corporate-style security.
3. The cost rises dramatically as company size increases, *without economy of scale* until a company reaches a medium size. If a 'large' company of 250 employees were to implement cyber security at the price paid by small companies (£110–500 per person), they would be paying £27,500–125,000 per year. Survey respondents with medium-sized companies of up to 249 employees set their maximum budget at £10,000.

3.2.3. Financial resilience

With the increased level of interactions and specialisation by smaller companies, it is becoming more likely that small companies will have access to disproportionately large datasets. An example of this in our dataset is a small company with access to pseudonymised medical records pertaining to 10% of the UK population (approximately 6.4 million people). Unsurprisingly, the company took cyber security extremely seriously and, thanks to the advantage of their size and enterprise architecture giving them full system oversight, had developed a security model that was more holistic than many large organisations could achieve. The consensus was that they were winning business from the public sector because of their investment in security and their good track record.

Examples abound of large companies that have suffered high-profile data breaches yet have weathered the storm — despite short-term impacts in terms of reputation and share price, the companies have managed to 'move on'. Small companies operating at much higher risk do not have the same capacity for resilience and often serve larger customers with the resources to terminate contracts early. A serious data breach at the small company described above would have been catastrophic.

Financial resilience in the case of a breach becomes a major differentiator between large organisations and SSITUs, with one potentially being too big to fail and the other being too small to survive. Thus far there has been limited UK press interest in breaches in SMEs.

As well as the increasing impact of breaches, the impact of the time required to remediate is greater in small organisations with fewer staff to share the task and continue operating, meaning that, with sufficient knowledge, they should hold more incentive to secure than their larger counterparts.

3.3. The knowledge vacuum

Our participants described two problems related to knowledge: a general awareness of cyber security and the subject matter expertise of the security decision maker/implementer.

3.3.1. Security awareness

Concern over the level of cyber security awareness came mainly from the RH and SP stakeholder groups. There is a large quantity of information provided to SSITUs about basic security measures[7], which one participant stated had impacted on security practices by individuals and families, but had less impact on small businesses. Participants also described a general evolution in the level of security awareness possessed by non-technical company executives.

In line with the suggestion made by Renaud [14], advice has become more consistent over time. However, given our participants' descriptions of the other constraints faced by SSITUs it is unsurprising that small businesses are finding security advice more

[7] See, for example, `www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary`, `www.gov.uk/government/publications/cyber-essentials-scheme-overview`, and [13]

difficult to assimilate into their organisations. Despite stakeholder concerns, none of the small businesses described by our participants lacked an initial awareness of cyber security threats; they were struggling with the more complex demands of quantifying and treating the risk.

One participant did talk about the growing fatigue he felt towards security, questioning the effectiveness of the measures he was advised to implement, making the point that these measures may just be current fashion. These comments may indicate that the awareness of SSITUs has a lifespan — there may be time constraints on SSITUs forming better security habits.

3.3.2. Security expertise

The majority of participants in the smallest organisational structures (single person, micro-companies and families) highlighted the need for 'DIY' cyber security — resource constraints within small organisations mean that this type of business process needs to be completed in-house by an existing member of staff. Self-reliance is a facet of entrepreneurship — "considerable initiative" is one of an entrepreneur's defining characteristics[8] — and Lazear [15] suggests that a defining characteristic of entrepreneurs is a broad skill-set, without being a subject matter expert, allowing them to adopt a variety of roles within their organisations.

There are conflicting views on how this decision maker characteristic might influence the quality of security employed. In their study on self-efficacy in cyber security Rhee et al. [16] suggest that confidence encourages security adoption, whereas the stress of an incident reduces self-efficacy. In the responses we received from SMEs there was a link between participants having no security expertise and their confidence that they could apply suitable measures. This could be analysed as complacency or the entrepreneur's typical reaction to a challenge. Van Eeten and Bauer [17] suggest that the measures selected depend on the decision maker's knowledge and one participant admits that the results of this DIY approach are "very hit and miss" in terms of both IT security and IT in general.

The results of our study suggest that confidence reduces as the level of research and knowledge increases; this indicates that, beyond a certain degree of security (perhaps the difference between securing a home user and a small company), a non-technical decision maker gains sufficient knowledge of the problem to lose self-efficacy. Dang and Pittayachawan [18] suggest that self-efficacy is improved by a supportive environment, reducing the pressure on the non-expert to find a solution when an incident occurs.

Understanding what measures to deploy and implementing them, as well as understanding how to act or react within their system, were both highlighted as a challenge. Without sufficient knowledge, participants struggle to understand and prioritise risks, and doubt their ability to remediate should they identify a problem. Some emerging systems, such as consumer cyber-physical systems, are so complex that the large suppliers involved in their implementation indicated having difficulty evaluating security requirements, highlighting the level of challenge the SSITUs would face.

The need for DIY security, combined with low knowledge and a lack of redundancy in security staffing — even in larger SSITUs — makes usability a key attribute of any security tool used by this sector. Some participants mentioned limiting the number of suppliers they used as a means of reducing the quantity of knowledge they required and improving automated interoperability. Many of these easy-to-use services make privacy and confidentiality by default difficult [19]. In the case of stand-alone security products, participants highlighted that 'free' products require considerable configuration, which, when combined with Wynarczyk et al.'s definition of small businesses as 'price-takers' [10], means that the cost of individual security measures may be too high for some SSITUs — the time burden of configuration is greater than equivalent product costs.

3.3.3. Peer-support

There is a scarcity of cyber security experts[9], and this influences how affordable their skills are for SSITUs. Participants highlighted how government accreditations such as Cyber Essentials Plus[10] make experts too expensive for SSITUs.

Our data indicated that, in the event of an incident, SSITUs' access to support may depend on luck, as they lack budget for employing security experts. There were several mentions of more organic routes taken by SSITUs to gain advice about cyber security.

The interviews with micro-organisations and an innovation centre suggested that very small companies have some free mutual exchange of expertise on subjects like cyber security where no expert is present, in an attempt to solve problems without cost to their community. Charities and clubs look for professional support from volunteers who will treat their involvement as corporate social responsibility; a consequence is that charities may have to reduce security requirements to get the IT services they need.

We propose that the lack of direct access to experts, combined with the lack of budget and the DIY nature of many small businesses' IT systems, may lead SSITUs to seek inexpert support. In the case of family members and acquaintances, any poor advice is unlikely to be malicious — although mistakes made during remediation could be as damaging to business

[8] www.dictionary.com/browse/entrepreneur

[9] www.ft.com/content/4cabd0fe-8940-11e5-90de-f44762bf9896

[10] www.gov.uk/government/publications/cyber-essentials-scheme-overview

continuity as the attack. However, it is not unrealistic to assume that users used to fending for themselves will also use the internet as a source of support, exposing them to malicious actors.

3.3.4. Outsourcing

Outsourcing, typically to the cloud, is often suggested as a solution to many SSITUs' security problems. One of our participants recommend that SSITUs should invest in automated systems that allow them to increase security without gaining knowledge. Our study indicates that IT and security are often synonymous in small organisations and the expectation is that support (and more broadly IT services) is free — there is often no remediation plan.

Outsourcing does not change the need to demonstrate a good understanding of cyber threats and good practice (especially if the SSITU is a data controller).

Our data indicates that the greatest risk from outsourcing IT and cyber security was a lack of understanding of the consequences and limitations of the agreed contracts. One of the biggest issues highlighted by participants was the use of web developers, etc. on one-off contracts, making the developer more likely to produce an unstable product that has customised the underlying platform to a point where updates are impossible or delayed. This risk is reduced by a decision maker's ability to ask knowledgeable questions when negotiating a contract.

SSITUs are unlikely to have enough specialised IT expertise in-house to undertake tasks such as developing web pages. Participants felt that the risk of outsourcing the hosting of a website, email, etc. to a third party is lower than that of contracting a developer to produce a website as a one-off project — reasoning that the ongoing relationship should motivate the supplier to create a higher quality product.

One RH participant highlighted that outsourced IT reduces the incentive to report incidents, which in his large organisation produced a security monitoring requirement that ensures performance is maintained. This position has been adopted as security is not easily outsourced — the risk is still held by the company, although the supplier accepts some reputational risk in accepting the contract. This option is unavailable to SSITUs due to the lack of resources to staff a 24 hour security operations centre and a lack of influence over their suppliers.

For SSITUs, even without the ability to monitor their systems, outsourcing certain elements of IT over the long term may be a better option than the alternative, as the large-scale measures employed by service providers should provide far better protection than the user can implement for themselves. A disadvantage is that these measures do not secure the user against the cloud provider itself, so the user has to trust the cloud provider's terms and conditions.

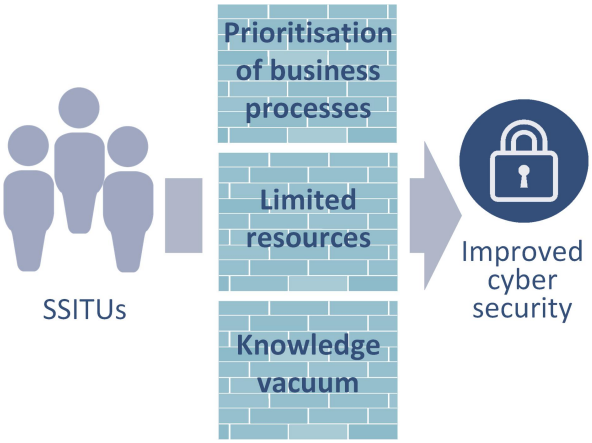


FIGURE 1. Contextual barriers to the implementation of cyber security

Before considering security investment, there are a number of barriers for SSITUs to overcome; this is summarised in Figure 1. These constraints limit the ways in which cyber security can be implemented by SSITUs before they begin to evaluate risk or consider the mitigations available to them.

In the next section we explore the risk assessment process, evaluating how the operational context provided in this section relates to the ability of SSITUs to apply a risk assessment process.

4. IMPLEMENTING THE RISK ASSESSMENT PROCESS IN A MICRO-ORGANISATION: AN EXAMPLE

In this section we evaluate current risk assessment (RA) processes against the decision-making context described in Section 3, both as a means to test the adaptability of the process for SSITUs and to frame discussions around SSITUs' understanding of their digital assets, the cyber threats they face, and the level of risk they are typically accepting. We start by discussing which SSITU groups would be interested in undertaking a risk assessment and the current practices described by SMEs. We then provide a micro-company scenario, based on a composite of IT system descriptions from our participants, as means of illustrating the RA process.

RA processes typically have a number of common stages (albeit with the sequence varying between authors), involving identifying: participants; the scope of the system under assessment; the vulnerabilities present in the system; the threats to the system, their likelihood and the impact of this happening; and the treatment of identified risks. With the exception of the identification of vulnerabilities (which is excluded by the more lightweight processes aimed at smaller organisations [20]), we will use these stages of the risk assessment process to structure our discussion of the results from our study that relate to the identification and prioritisation of risks (Sections 4.4–4.6). Finally,

in Section 4.7 we discuss the risks faced by those SSITUs identified in Section 4.1 as not needing the risk assessment process.

4.1. SSITUs' need for RAs

The SSITU group encompasses a variety of subgroups, with individuals potentially having multiple roles in several other SSITU groups, or potentially being an employee of a large organisation. Although all subgroups will have some cyber security risk to treat, the application of a formal risk analysis process would not be appropriate for some groups.

We divide the groups based on their propensity to employ other types of formal business process in their organisation. This is not limited to businesses — small charities need sufficiently rigorous processes and some private clubs will have to justify their processes to their members.

There was evidence in our study of SSITUs who were *advice-takers* (implementing some security based on government, supplier or peer-support network recommendations) and those who were *risk-evaluators*, who attempt to correlate the security they implement to the risks they face. As well as the split between business/charities and privately used systems there was also a slight distinction between industry sector — by accountability and the commercial importance of their IT system.

As the groups become less accountable to external parties — families and individuals, for example — there were fewer recognisable business processes employed, making a formal RA inappropriate. However, even in a family context, there is evidence from our participants that some kind of RA is being employed by the nominated IT expert, in order to protect vulnerable users and home working activities. They indicated that these decisions are based more on the understanding of common security practices held by the 'expert' than a risk-based strategy, moving a no-security system towards a perceived benchmark.

4.2. Current practices in SMEs

Despite the key role that risk analysis plays in the cyber security lifecycle, the majority of the SSITU participants in our study did no formal RA. This is unsurprising for individuals and families, but the initial questionnaire dataset, which focused only on SMEs, also described a lack of formal processes — some statistics from the questionnaire can be found below.

That over half of SMEs had not included cyber security in any form of risk analysis is a source of concern for the RH stakeholder group.

Irrespective of whether a participant had carried out a formal RA, the SME questionnaire asked respondents about the types of risks they faced. Although a small sample, the respondents were from a broad range of sectors, company sizes and areas of the UK. The categories of risk used in the questionnaire are displayed in order of frequency of response (from 94% to 0%), providing an initial indication of the things most likely to motivate SMEs to engage with security:

- Sales being dependent on company and employee reputation (31 of 33).
- Having customer or supplier data to protect (27 of 33).
- Having intellectual property (IP) to protect (20 of 33).
- Having interconnected customer or supplier systems (19 of 33).
- Having a website containing input fields (14 of 33).
- Using predominantly social media for advertising (9 of 33).
- A risk of losing customers if they do not implement a cyber security standard (2 of 33).
- None had safety-critical systems.

As a whole, the responses to the risk analysis section of the questionnaire demonstrate that SMEs are aware of reasons why they should be implementing cyber security measures. But, using a participant's own words, the most difficult thing about cyber security is *"Knowing about the risk management requirements to keep the threats under control."*

There is also the wider issue of SSITUs distinguishing genuine information from what one respondent termed "scare stories", in order to provide a means by which to judge the impact and likelihood of a cyber attack. Without this information, SMEs would find it difficult to determine the most appropriate risk management strategy.

Outside of the IT, telecoms, security and defence sectors (for whom security would typically be a product), SSITUs in our study conflated the definitions of risk, threat and vulnerability. Although this would not have enormous relevance to their informal assessments, it means that in some cases we will use the term 'risk' interchangeably with threat or vulnerability to accurately represent comments from our participants.

Some cyber security experts may regard this as an indicator of either a lack of knowledge or the immaturity of security processes. However, this section is intended to describe how the risk assessment might align with the other business processes carried out by SSITUs and in terms of return on investment (for both the SSITU and any RH stakeholder who has requested it). Rather than asking *which common cyber security practices are SSITUs failing to implement*, the methodology encourages an evaluation of what they *are* doing, where constraints may make it infeasible to implement more rigorous processes and what impact that may have on the small-scale cyber security ecosystem as a whole.

4.3. Scenario

We use a scenario to support our consideration of the application of a formal RA process by SSITUs. The scenario combines the information given by a number of participants running micro-organisations to provide a realistic description of an IT system in a micro-company (employing fewer than 10 people). All elements of the scenario are drawn from real system descriptions, but no system was identical, so the use of this scenario allows us to highlight all of the most common attributes described in our dataset using a single example.

The scenario uses the example of a small accountancy firm that has one director and two junior accountants/administrators. The firm provides accountancy and bookkeeping services, mainly to other micro and small businesses. Staff work mainly from home, with the company director either arranging meetings at her home or visiting clients for meetings.

Although one employee was issued with a laptop, the other employee works only part-time and so uses his own PC. The director has a laptop supplied by the company, but has not purchased a second device for personal use. All three members of the company use their personal smartphones to check emails and talk to clients. The company also has a website, email server and various social media accounts, allowing them to advertise their services and be contacted by current and prospective clients. The website and email server were developed, configured and hosted by a small web development company.

Accountants have to handle a large quantity of sensitive information on behalf of their clients. Information is provided to the accountant in a number of formats, as imposed by the client — some email spreadsheets, some allow cloud access to accountancy packages and bank statements, some provide VPN access to records on their own systems, and a few provide original paper records. Management accounts are supplied to the clients both electronically and by post; completed tax returns are submitted to the UK Revenue and Customs Organisation (HMRC) via an online portal.

As the trading address for the company is the director's home there is very little IT infrastructure. Both the director and her employees rely on small office/home office (SOHO) routing, using devices supplied by the internet service provider (ISP). These networks are shared with other members of the employees' households.

Any work product passed from the employees to the director, or generated by the director herself, is periodically backed up to external hard drives, which are stored securely off-site. The company has no policy of using automatic or cloud backups for endpoints, but does transfer data via company email, all of which is backed up by the hosting provider. A network diagram illustrating the environment is given in Figure 2.

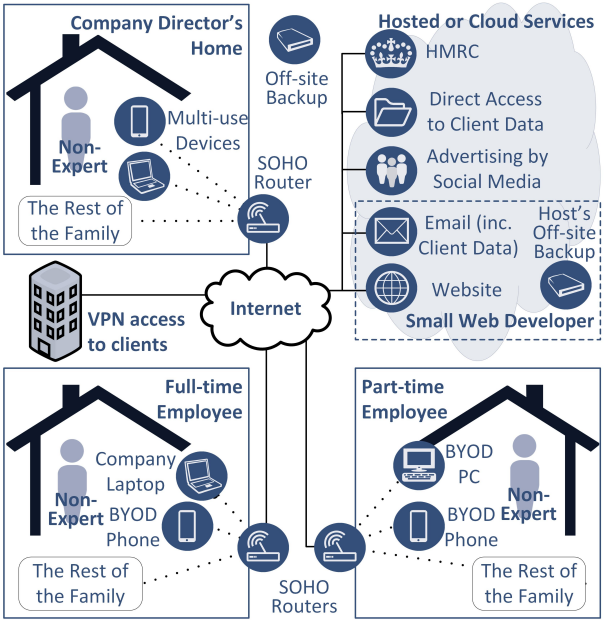


FIGURE 2. Scenario architecture

4.4. Scoping and engagement

4.4.1. The participants required for meaningful results
RAs are typically carried out by teams, although the authors of the more lightweight OCTAVE Allegro [20] state that it has been carried out by one senior member of staff "relying on their knowledge of the operational area" [20]. Typically, even Allegro expects there to be more than one person carrying out the analysis as a member of the IT team is needed to "provide technical depth that other members of the team may lack" [20].

Participation of multiple stakeholders in the RA process is not only to provide different types of expertise — the inclusion of multiple members of staff introduces a need to discuss requirements, increasing the breadth of risks identified [21].

Even if the company director in our scenario decides to include her two employees in the process, there is still no representative from an IT function and no participant with knowledge of the systems controlled by external stakeholders. Caralli et al. suggest that anyone new to the risk analysis process will need 1.5 days to become functional in the OCTAVE Allegro method; that analysis time relates to the number of information assets and system complexity, given that an assessment of the first asset may take the team several days [20]. This level of commitment — all the company's human resource for more than a week — is unlikely to be acceptable to the company director in our scenario, who will need to provide service continuity to her clients.

4.4.2. Defining a meaningful scope
The ultimate aim of carrying out a RA is to identify and prioritise risks for treatment so that an organisation can achieve the most security for their investment [2].

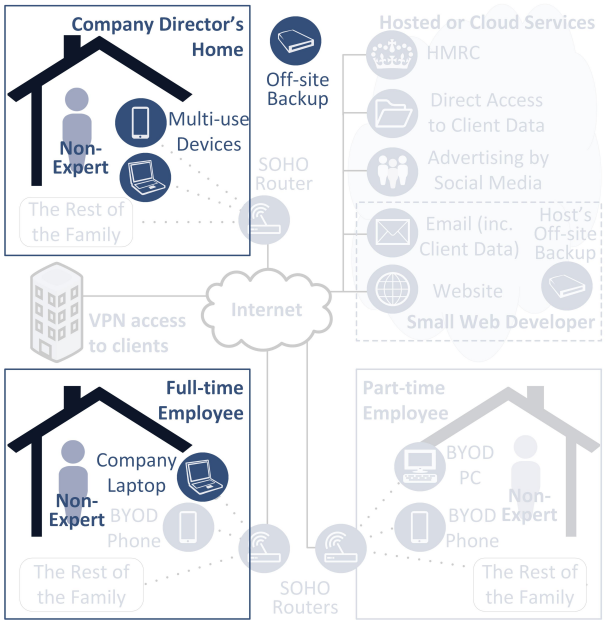


FIGURE 3. Decision-maker controlled elements of the scenario archiecture

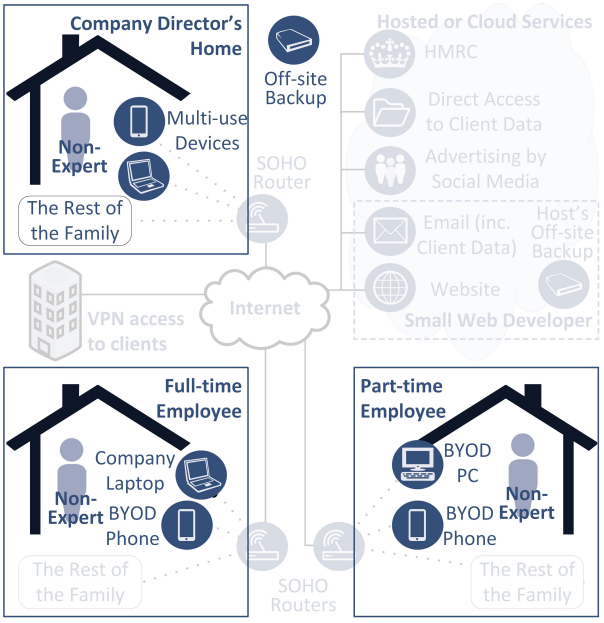


FIGURE 4. Decision-maker and IT policy controlled elements of the scenario archiecture

For this reason, and because the output of the process increases in complexity as the scope grows, the decision maker may decide to include only the elements of the system that are within their control.

This scenario is not only realistic, but may be perceived as good practice in the context of advice given to small organisations in the UK. For example, the first iteration of the aforementioned Cyber Essentials Standard puts cloud services entirely out of scope when advising on the application of security measures, due to a lack of user control. (One participant suggested that this standard is likely to evolve as more accredited "secure clouds" enter the marketplace.)

Applying this scope to the system in our scenario, the scope for RA is illustrated by Figure 3. As can be seen, the only elements the decision maker has sufficient control over, and to which she could add *effective* security measures, are the two laptops and her personal smartphone. (In this context, an *effective measure* is one that the decision maker can implement in the knowledge that no other system stakeholder can remove it without authorisation.)

This limited scope may lead to the implementation of some security measures, such as antivirus and automatic updates, which the majority of SSITUs in our study use. It may also explain why these types of basic measure are the *only* security measures the majority of the micro-organisations in our study have knowingly adopted.

The company may also be able to broaden the scope using soft-power — with their IT policy and by explaining the impact of security breaches both to the two employees using their own devices and to the decision maker's family, who share the home network with her company. This would increase the scope to include the devices owned by the two employees, and may reduce the likelihood of the business owner's partner or children introducing malware into the company network. However, as seen in Figure 4, it does not increase the scope to include the web developer due to the lack of knowledge described in Section 3. Nor does it increase the scope as far as the SOHO router — the SP and RH stakeholders in our study retain control of a significant portion of the infrastructure.

Although this scope may make the analysis simple enough to implement and so increase security for the organisation, an awareness of risks associated with uncontrolled elements of the system would provide context for processes such as disaster recovery planning. If the scope was expanded to include the elements of the system the decision maker is concerned about (for example, one of our participants stated concerns that "People are hacking accountants' login details to HMRC to submit false tax repayment returns"), it would then cover the entirety of the system illustrated in Figure 2.

The two stakeholder groups who are not exclusively SSITUs (RH and SP stakeholders) can influence the security of SSITUs. Our participants indicated that concern from large organisations is a bigger driver of change in small-scale cyber security dialogue than the concerns of the SSITUs — cyber risk owners for the access credentials or data held by SSITUs are not only the SSITUs themselves.

Our RH participants described how the inevitability of some compromises occurring leads to a need to consider cyber security in all activities, including interactions with other organisations: the risk to suppliers seems to become an incentive for them to

retain as much control over their shared systems as possible.

Even in small-scale IT systems there is complexity, with much of this complexity being created by the interactions between the different organisations who own the systems. Complexity in these interactions even limits the ability of SSITUs to test the quality of the security across their systems. For example, penetration tests can be carried out only where a system owner has given permission [22]. Even in the relatively simple architecture described in our scenario the number of system stakeholders would make the process prohibitively expensive, if not impossible.

Subashini and Kavitha [19] suggest that software as a service (SaaS) abstracts systems so that all a customer can see is a black box. When a system is abstracted to this extent, the system itself limits user incentive to acquire knowledge [23] — it is difficult for the user to gauge the quality of security and it is unclear how successful SSITUs would be in transferring the risk to their supplier.

This complexity gives rise to a diffusion of responsibility where some parties hold risk and other parties hold ownership or control. Roles and responsibilities between nodes become incoherent, which leads to gaps in security and inconsistencies in processes. There are parallels with safety-critical systems, where the most hazardous parts of the system are often where components interact and the responsibility for their safe operation is not clear. No stakeholder controls a sufficient proportion of the system to employ a Defence-in-Depth strategy autonomously.

The rising complexity in SSITUs' systems in terms of both the technology used and the number of intersecting service contracts means that SSITUs have a decreasing likelihood of being able to competently resolve their own IT problems. Kagermann et al. [23] would suggest that this is an intentional progression — that the abstraction of the mechanics underlying any technology is required in order to increase both the number of users and the number of technologies each user can learn to use.

Service providers have some legal responsibilities towards their customers, although it is not always clear how well these responsibilities protect consumers against cyber security risk, as in many instances case law is required to clarify how regulation applies. Providers also have some motivation to avoid any large, publicised breaches that would damage customer confidence — which may have a greater impact on overall security.

While in some sectors the risk is pushed onto the end user, our participants highlighted other sectors where the supplier assumes far more of the responsibility for cyber risk than the customer. For example, a law enforcement participant described how a need as an industry to protect consumer confidence in a service leads banks to be more willing to share or assume cyber security risk.

Software providers are also moving towards a service model ensuring that they retain contact with their customers, control of their software and most importantly access to data [23]. In these complex systems one might assume that responsibility to secure becomes a collective action; however, as Cialdini [24] highlights, moral incentives are poor motivators. It is difficult to find an incentive to secure when the victim is not the organisation in control of vulnerability, compounded by the differences in definition of an *adequate* security budget across the supply chain.

The participants in our study who would have traditionally provided IT support described a rise in the number of SSITUs contacting them in an attempt to obtain free support post-incident. This would indicate that cheap cloud services are only fulfilling a limited selection of the SSITUs' requirements — those which are the least complex to provide in bulk without flexibility.

The ability to advise SSITUs requires good visibility of threats, but threat intelligence is hard for SSITUs to produce as they have limited funds or IT knowledge. The UK government takes responsibility for offering simple advice to SSITUs (their incentives for doing so are discussed in Section 6). One of the key responsibilities our participants stated government bodies (in particular law enforcement) had accepted was one of encouraging SSITUs to take responsibility for their own role in cyber security.

Some decision makers in our study felt that holding responsibility for cyber risk inside of a company was the most appropriate solution — even if the risk was not reduced it was at least measurable, with the RH retaining control of all of their assets and reducing interactional complexity. One participant went as far as to use only in-house hosting facilities. The cost of unmitigable risk remains high, but in some instances retaining control acts as a measure for risk reduction.

A problem for SSITUs is one of bandwidth — they lack the resource to combat complexity with knowledge. Van Eeten and Bauer [17] question the ability of users to keep up with evolving threats. This concern was repeated by the safety expert in our study, who questioned users' liability or responsibility for safely using technology given their limited ability to understand the implications of the decisions they make.

Finally, liability is limited by legislation (see, for example, *The Blue Guide*[11]), and this attitude will extend to risk-accepting decisions within the supply chain. The number of degrees of separation in the event chain leading to financial losses changes the extent to which a supplier can be held responsible.

Defining a meaningful scope for a risk assessment can be challenging for SSITUs with such limited control of their systems. This issue is compounded by the limited

[11] ec.europa.eu/DocsRoom/documents/4942

knowledge (as described in Section 3), which could limit the extent to which SSITUs are able to select a scope based on an understanding of threats (discussed in detail in the following section), or the potential breach impact that the decision maker believes the company faces.

4.5. Identifying threats

In their qualitative risk assessment process Alberts and Dorofee suggest identifying cyber security threats to critical assets [21].

Understanding threats was highlighted by our participants as one of the most challenging aspects of cyber security. Taking the most prevalent response given by our SSITUs, our scenario company director would struggle to assess the threats her company faces due to a lack of understanding of *why* attackers would be motivated to attack her and the limited SME-relevant threat intelligence.

Sections 4.5.1–4.5.7 summarise the difficulties that our data has highlighted SSITUs have in identifying threats, as well as discussing the various types of threat a cyber professional would recognise and their applicability to our scenario.

4.5.1. The availability of threat intelligence for SSITUs

Data feeds about threats faced in certain sectors are available from CERT[12]. This was one of the services highlighted by law enforcement when notifying hosting companies about persistently compromised machines. Feeds such as this, or data that can be purchased or accessed from other sources, may contain the threat information that SSITUs need, but may not be in a suitable format for low-knowledge users.

The Information Commissioner's Office (ICO) provides some data and a quantifiable risk for not maintaining 'adequate' security in the form of penalties, but they only publish the details of the worst incidents in their penalty notices[13].

Incident reporting provides statistics for handling cyber security, but our participants indicate that small organisations see little benefit in reporting cyber incidents. Threat intelligence held by CERT, specifically about small organisations, was mainly from the Cyber Security Information Sharing Partnership (CiSP). CiSP is a safe, moderated environment for exchanging data, but the branding may act to dissuade small organisations and the majority of current users are exchanging technical information (such as IOCs[14]) not readily consumable for SSITUs.

SSITUs in our study used peer-support to remediate when incidents occur. At the point that they are looking for the type of information CiSP holds, they may well be facing the time constraints of actively needing to remediate. CiSP need to verify the identity and affiliation of new members before they join, but the time and credentials needed for this may make unmoderated forums or inexpert friends more readily accessible.

This brings us back to the problems faced by SSITUs when searching for free security advice described in Section 3: SSITUs need to understand the cyber risks relevant to their systems, but also the risks that different post-incident actions might represent.

4.5.2. SSITUs' understanding of threats

A sizeable minority of participants in the study stated that credible evidence about the magnitude of the cyber security problem would be instrumental in their deciding to implement security measures. In order for them to properly understand risk they needed a better understanding of why small-scale IT systems might be appealing to an attacker.

As discussed earlier, vulnerability analysis has been excluded from our discussion of the RA process in line with the lighter OCTAVE Allegro process [20]. Vulnerability analysis highlights the attack vectors potentially available for exploitation, depending on the knowledge, skill and resource available to the attacker [21]. In RA processes that omit this stage, the decision maker has to evaluate risk based on an abstract understanding that their systems *could* be vulnerable and that they have identified threats — that they have identified the incentive an attacker has to target a specific system or set of systems, which feeds into the measure of the likelihood of attack.

Risk is defined by the value of an asset to *anyone* — the owner has a potential for financial loss, and/or an attacker has something to gain [2]. This is in contrast to privacy issues, where the decision maker is attempting to protect an asset due to its sensitivity — the owner does not want to suffer a loss in confidentiality that could, for example, alter their standing in a community.

Our study highlighted that people involved in providing security advice to SSITUs were often told that an individual or organisation had nothing of any value to protect. This was replicated in our interviews with SSITUs — even those with considerable security knowledge. This attitude towards security was adapted when the question is reversed and SSITUs are asked if they are willing to make all their data open-source. Even if there are no critical assets such as intellectual property to protect, SSITUs still feel that their data is "not anyone else's business."

A variety of threats can be posed to computer systems, depending on what an attacker is trying to gain in targeting a system, or the natural, environmental or operational events that could damage the system [22]. This is where SSITUs in this study had the greatest

[12] `www.cert.gov.uk`

[13] Information Commissioner's Office: Action we've taken: `ico.org.uk/action-weve-taken`

[14] `www.openioc.org`

difficulty in measuring their own risk.

Low-knowledge participants voiced concern over the lack of data to support decisions, but more fundamental was the issue of understanding cyber security from the perspective of the attacker. Renaud describes a number of psychological reasons why SMEs might choose to avoid taking security threats seriously, which align with our comments in Section 3 about resources and ability, and how advice is muddied by inconsistency [14].

Throughout this paper we highlight some genuine barriers to decision making, but the psychology of the decision maker cannot be entirely dismissed. As low-knowledge technology users, many of the participants were asking *why would I (as an individual or an organisation) be attacked?* The qualifications that participants use when this question is raised suggest that the question they are actually asking is much narrower: *why would an attacker choose to target my role or organisation?*

As they don't have much knowledge of their IT system, the value it contains, or the ways in which it could be exploited, they are focusing on the easier question of why an attacker would have an interest in them in particular — they are not asking *what does an attacker have to gain from having access to my system?*

The more knowledgeable participants were able to define forms that a targeted attack might take and what artefacts they might find post-attack. However, participants unanimously agreed that they hadn't been the subject of any form of highly-resourced, focused attack. Those who had seen evidence of cyber attacks against their organisations felt that they were 'run-of-the-mill'. This may go some way in explaining the lack of a sense of urgency SSITUs display when considering the potential vulnerability of their systems.

4.5.3. Targeted attacks versus targeting organisations: defining 'targeted attacks'

Targeted attacks occur when attackers are willing to devote large resources on a single target. Li et al. describe advanced persistent threats as:

> "a cyber attack launched by a group of sophisticated, determined, and coordinated attackers who systematically compromise the network of a specific target machine or entity for a prolonged period." [25]

The dataset describes a number of tactics, techniques and procedures (TTPs) that interviewees felt could vary the sophistication of an attack:

- The amount of time it would have taken to develop a sophisticated attack and how specific this attack is to a unique target.
- The value of the exploits used — has the attacker used zero day exploits or a set of widely available exploits?
- The number of iterative steps required to carry out an attack, a lack of automation or having a human in the loop — law enforcement participants highlighted the use of employees on the back ends of spoofed websites to enter captured bank details into real banks' websites as part of some higher value attacks.
- The quality of the social engineering aspects of an attack, or the accuracy of communication — has spam been sent to every possible email address at an organisation's domain, or only to specific employees or mailing lists?

Any of these TTPs could indicate a greater motivation to gain access to a system; however, the SSITUs in our dataset showed no *awareness* of targeted attacks. Either SSITUs' low quality security measures provide unsophisticated attack vectors, they have no way of detecting sophisticated attacks, or none of the low-knowledge participants in the dataset held particular interest to well-resourced hackers.

In the case of our scenario we do not expect the accountancy firm to be subject to a targeted attack. Hypothetically, the only reason that a company of this size and type might sustain a targeted attack is if they were acting on behalf of a public figure, or an organisation whose activities are controversial. One participant, who owns an IT support company and has a high level of technical knowledge, described his choice *not to accept contracts from perceived high-risk clients.* There is also some evidence of targeting given by small NGOs, often with political activities [26].

Although SSITUs did not report being victims of sophisticated targeted attacks there was some evidence of attackers targeting one or more SSITU user groups. In these cases the attacker will not have invested the resource required for targeted attacks, but still has an objective, rather than just acting opportunistically.

One example in our dataset described the use of cyber attack as revenge, highlighting how cyber security is seen to be a weakness in small organisations:

> "We have come under attack from Far Eastern and other competitors due to legal action taken by us in connection with Intellectual Property"

Sections 4.5.4 and 4.5.5 discuss the different assets an attacker may be focussing on when attacking a system.

4.5.4. Data that are interesting to an attacker

The main threat incentive described by our participants was fraud — characterised by gaining access to a victim's bank accounts, identity theft and credit card fraud.

An asset that holds a value can become a threat incentive if there are insufficient security controls to discourage an attacker (and the data economy has ensured that all data has value to somebody). Subashini

and Kavitha suggest that the value of data is a function of its quality [19].

One reason why our SSITU participants feel that they are less at risk of a major breach is that they don't hold sufficient volume of these valuable data to entice an attacker. However, our scenario accountant should be concerned as the data they hold is often sufficient for an attacker to access bank accounts, etc. Despite its limited quantity, the quality of the data could motivate an attacker to target our scenario company — there is already precedent for larger accountancy and legal firms to be targeted[15].

In contrast, given the correct circumstances, SSITUs may hold more attractive data than large organisations. One example is that of IP, which SSITUs lack the resources to try and protect via legal process, meaning that IP stolen from small organisations has a more persistent value to an attacker. As previously discussed, one participant had not only suffered a loss of IP, but also suffered subsequent cyber attacks, which would have caused financial damage — further reducing the capital available for legal defence.

4.5.5. IT systems that are interesting to an attacker

When the IT resource itself is the asset, the SSITU may overlook its value to an attacker. For example, SOHO routers have been shown to be vulnerable[16] — a law enforcement participant also gave an example of victims they had notified about a breach they were part of as a result of a botnet predominantly focused on hosted servers.

If an attacker is looking for a platform with high uptime, then the aforementioned SOHO routers are a good target as they may not be unplugged for years. Network connectivity and bandwidth would also be valuable; however, the most important attribute is *persistence*. Improvements in distributed computing and the fact that many activities such as spam relays don't require high-powered computing inevitably increases the appeal of having control of large numbers of low-power but persistently compromised devices.

Our scenario company should be concerned about this type of threat as it could prompt an attacker to access a network holding customer data, either forcing the company to report a breach to their clients, or disrupting their access to services. Worryingly, while high-knowledge participants, such as IT service providers and a law enforcement participant, were aware of this type of persistent breach being an issue for SSITUs, low knowledge participants showed no awareness of this type of threat.

[15] "Lawyers and accountants are prime targets for cyber attacks" `www.ft.com/content/f52f6fee-ccf4-11e6-864f-20dcb35cede2`

[16] `www.team-cymru.com/ReadingRoom/Whitepapers/TeamCymruSOHOPharming.pdf`

4.5.6. Opportunistic and nuisance attacks

The majority of high-knowledge participants mentioned observing *opportunistic* attacks on their systems: the ease with which these are detected led one participant to call it "background noise" — although SSITUs with no security measures may still be vulnerable. These types of attack could be described as using uniquely low value commodity threats.

Vulnerabilities become so widely known that exploits are available in certain online marketplaces, made usable for novice hackers looking to gain from IT users who are behind on updating their systems [27] — exploits are becoming commodities.

The examples of opportunistic attempts given in our dataset include spam/network attacks using malware easily detected by antivirus, spam friend requests on social networks, unauthorised Wi-Fi users, and pre-compromised 'free' software components.

These types of attack could also be categorised by the level of knowledge and effort the SSITU is required to have to avoid them — a combination of taking 'essential' measures, such as those advocated by a scheme such as the aforementioned Cyber Essentials, and managing expectations (ensuring that users ask themselves why software is free), practically eliminates these types of threat.

In line with the outsourcing discussion of Section 3.3, the small proportion of participants relying on the type of IT outsourcing that gives them regular access to experts were advised to implement essential measures, although possibly not routinely updated about scams. Those using cloud services with a small amount of support at a distance described more general requests for advice, from their professional networks and internet searches, more in line with the ad-hoc peer support mentioned in Section 3.3.

4.5.7. The evolution of threats

Cyber threats are evolving; some would suggest the attacker capability is increasing at a greater rate than companies are improving their security [13]. This evolution of threats and the corresponding arms race may have protected small organisations with poor security to a certain extent, as it means that there continues to be good returns from attacking the highest value targets.

SSITU participants suggest that benchmarking inside of their immediate community influences their decisions, meaning that the security of a community may depend on the availability of experts/security-aware acquaintances discussed in Section 3. The ability to be "slightly better than average" can be limited by resource constraints and the types of infrastructure used by a company, but it may provide an incentive when they select cloud service providers.

Our study indicates that some SSITUs have very large digital footprints, finding it difficult to separate

their digital work and private lives; in particular, owners of micro-organisations such as the company in our scenario have very complete open-source profiles.

SSITUs in our study knew there were large amounts of information about them online. This would make them good targets for social engineering, with low awareness of current scams increasing the attackers' chances of success. Increased connectivity and increased IT use by SSITUs provides this information to attackers and small organisations' reliance on online services increases their vulnerability.

Small organisations in general are seen by RH and SP stakeholders as being behind in the security arms race, but the fact that it is an arms race may act as a disincentive to SSITUs who perhaps feel that their efforts will never be good enough. As we discussed in Section 3 self-efficacy has a big influence over SSITUs' decisions, a concept backed up by Renaud, who describes the reasons why SMEs might reduce their perception of a risk they feel unable to treat [14]. The vulnerability of some small organisations might make them appealing to a certain type of attacker.

The risk to smaller organisations may develop as exploits reduce in value and enter the commodity threat market. The SSITUs in our study do implement basic security measures such as automated updates, but the limited control they have over some system elements, the reliance they have on product security and their low knowledge/resource mean that they may be slower at patching known vulnerabilities.

We hypothesise that security experts' knowledge about both threats to larger organisations and the cyber exploit marketplace may be used to produce more proactive security measures for small organisations — if small organisations don't warrant a high-investment from attackers then there may be more time for SSITUs to react to emerging threats before they become relevant to organisations of their size and value. If they begin patching vulnerabilities at the same time as larger organisations they could protect themselves before a threat evolves to apply to them.

A summary of how our dataset represented threats to SSITUs is illustrated by high-level misuse cases in Figure 5. Threat is an element of cyber security that smaller organisations have particular difficulty understanding. There is not enough accurate, accessible and SME-relevant data available from credible sources to assist decision makers. When combined with the low resources discussed in Section 3, it becomes obvious why SMEs in particular stated that there was often not enough evidence to warrant much investment beyond installing antivirus.

However, it is also worth mentioning that once identified, threats are used in a very specific way by a risk assessment process. In the case of [21] an estimation is made of the level of threat based on the capability/resources of the attacker. If this is then used to contribute to an estimation of the likelihood of an attack succeeding then the capacity of the victim to resist the attack has to be measured in relation to the capability of the attacker — the constraints outlined in Section 3 make *all* threats, from script kiddies to well-resourced knowledgeable actors, more difficult to repel.

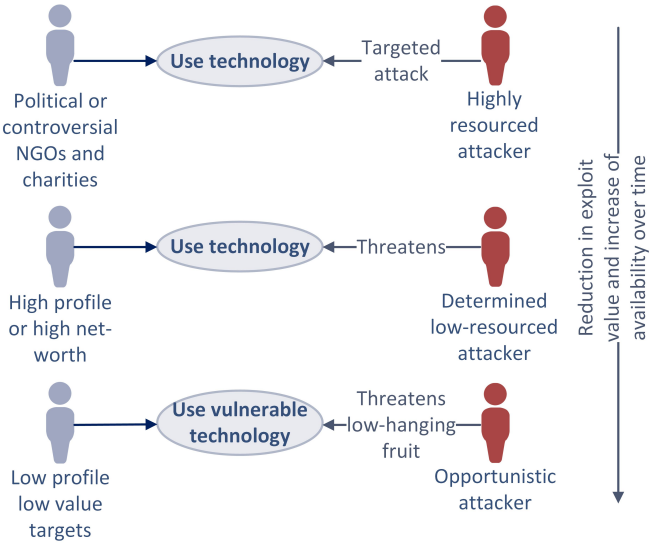


FIGURE 5. Misuse cases concerning different SSITU groups

Experts' knowledge of threats in the provision of advice to SSITUs may be highly effective in reducing SSITU vulnerability, but in the context of a risk assessment carried out by the non-expert SSITU director in our scenario, enumerating threats that all have the same *high* threat level may not provide sufficient value to the SSITU to warrant the time invested.

4.6. Calculating and treating risk

In a process where vulnerabilities are excluded (such as [20]), and where an SSITU's resources are sufficiently constrained so that all threats are relevant, risks will be calculated largely on the harm that the SSITU would sustain in relation to the reduced confidentiality, availability or integrity of various assets. This may explain why the majority of SMEs made no mention of a formal risk assessment, but were still likely to implement backups. The harm caused by the loss of an asset aligns with pre-existing disaster recovery processes, where quantifying the harm caused by a lack of confidentiality is harder to estimate.

If threats discuss what an attacker has to gain from a breach, then risks highlight what the SSITU has to lose in the breach. Based on our data, the scenario company is likely to define risks relating to the following themes:

- protecting company reputation and ensuring that the company's public profile is both available and as intended;
- protecting customer data in various locations;

- protecting the home network;
- the physical security of devices and the backup drives;
- the continued availability of internet connections and reliable function of devices;
- protecting valuable credentials, such as login details for the company website, HMRC, and social media accounts; and
- protecting their customer systems when given access via cloud applications or VPN.

The three members of the company in our scenario would find it easy to apply endpoint security measures, and the company director paying for a subscription to an antivirus provider for the casual employee would probably be wise to ensure that his PC had the same measures as the company-owned machines. The director could also implement a policy that all devices are configured to automatically accept any security-related updates.

These measures, in combination with the regular backups the company is already employing, represent the benchmark of typical security measures employed by the majority of our SSITU participants. In terms of risk treatment, these measures should reduce the general cyber security risks to the *controlled* portion of the system, moving them towards the aforementioned Cyber Essentials standard and making the scenario organisation less vulnerable to opportunistic attacks.

All the other risks identified for our scenario company are subject to limitations on the risk treatments available to the decision maker. The company director doesn't control the platforms on which these services operate, so service providers implicitly become SPs for their customers. The only proactive measure the decision maker can take independently (and which most participants already do) is to develop a recovery plan should a security breach occur.

Beyond this, we would suggest that risk treatment is dependent on the perceived responsibilities of the various supply chain stakeholders, whether contractually or legally defined, or evaluated in terms of reputation-protection.

In Section 4.4 we discussed how system control influences the scope chosen for a RA. There were obvious control constraints for the SSITUs who participated in our study, although virtual organisations are those who have the greatest issues, by not owning any of the devices or networks through which their activities are carried out. The constraints SSITUs face influence their ability to treat risk, irrespective of its impact, meaning that SSITUs may be demotivated to attempt good security practices as they don't have any real influence or control in the system.

In the examples provided by our participants, system control depends on ownership or holding power in the relationship with the owner. Risk ownership was described independently from device, system or data ownership, and — often due to the complex interactions between supplier systems — the risk is not held by the system owner.

Big corporations influence the sector by the service level they are willing to offer — one participant highlighted how important being cost-effective was to providers, leaving little room for customers (large or small) to negotiate. Most participants, however, were focused on soft-power options for increasing cyber security capability in small organisations — finding ways to encourage suppliers to improve security such as making a business case, rather than using legislation to strong-arm compliance.

As well as a lack of control over the systems decision makers use, this analysis of the risk assessment process indicates that the current entry-level options for SSITUs are difficult to apply to a very small organisation. The different approaches offer differing levels of difficulty, producing a kind of pathway that could allow a business to incrementally improve their security. However, while these would work well in a larger organisation with no formalised cyber security process, the first stage possibly represents too large a step in terms of the time required or the level of knowledge a SSITU would have to acquire.

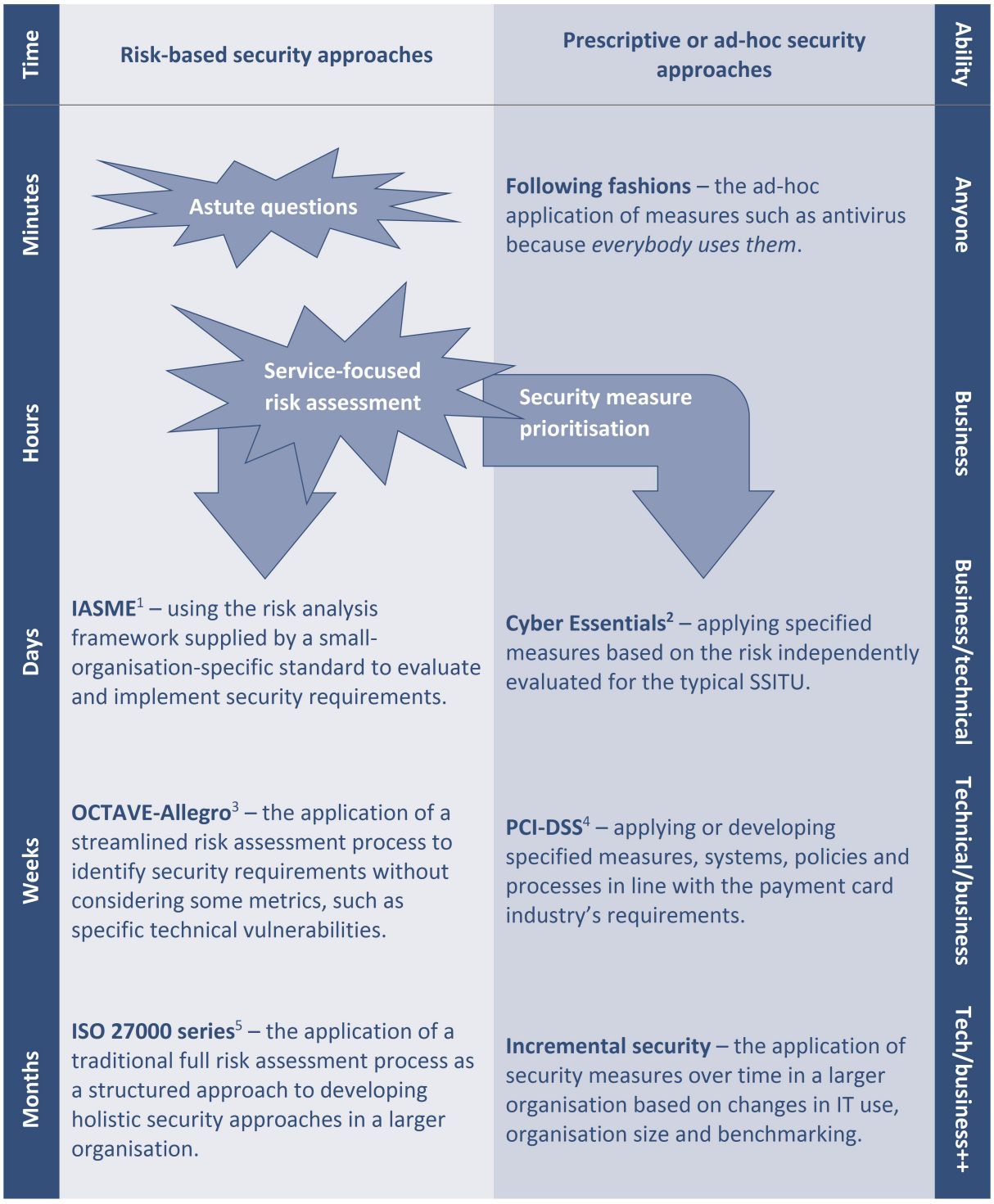
However, there is also a gap in the alternative 'prescriptive' or 'ad-hoc' pathway described by our participants, between the ad-hoc application of cyber security measures such as antivirus and the implementation of a scheme such as Cyber Essentials. These pathways are illustrated in Figure 6.

The gaps in both pathways mean that there is no smooth progression between the 'basic' measures our SSITU participants have applied without much knowledge and the next available step, due to the increase in both time and knowledge required. Some SP participants had already begun asking SSITUs the 'astute questions' we feel are the first step on the risk pathway. But, to bridge the gap or facilitate the prioritisation of measures, which would allow SSITUs to bridge the gap between ad-hoc measures and the Cyber Essentials standard, we feel that a lightweight service-focused risk assessment could be useful to some SSITUs. As part of implementing the standard, IASME[17] offers an equally lightweight assessment, but the interaction required to obtain this might represent too great a commitment for some SSITUs.

For those SSITUs wanting to justify security investments, rather than simply accepting advice, the initial steps required in either pathway may be too difficult to attain in a single increment with the level of knowledge they hold — a lack of intermediate steps could be limiting cyber security self-efficacy.

The scenario we presented in Section 4.3 was by no means a worst case scenario for risk in the SSITU group. We identified two types of *high risk SSITU* based on

[17] www.iasme.co.uk



[1] https://www.iasme.co.uk/
[2] https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
[3] http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=84
[4] https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security
[5] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=66435

FIGURE 6. Gaps in the entry-level options on pathways for SSITUs increase cyber security

comments made by our participants:

1. The charities or public figures mentioned in Section 4.5 who are at risk of targeted attacks, potentially by well-resourced actors (nation states) depending on their activities.
2. Entirely virtual organisations.

Our study indicated that, as well as the size and resources of the organisation, there were a number of other constraints and incentives that could influence how *formal* their IT processes and policies became:

- The market value for a SSITU's time.
- The larger and well-established SSITUs tend to have an IT function and are working towards a large corporate IT model, whereas larger virtual organisations will have distributed responsibility across the different services they have contracted.
- Existing practices — in sectors such as manufacturing (or, as another participant indicated, industries involved in audits) standards are treated as just a part of doing business, leading to resignation, rather than outright rejection of the idea that cyber security standards may be pushed down the supply chain.

Although applying standards may align with some SMEs' other business processes, we saw no evidence of decisions related to other constraints discussed in Section 3 — resource or knowledge — being overridden by regulation in cyber security.

4.7. Risk for other SSITUs

As outlined in Section 4.1, a proportion of our SSITUs will never feel the need to assess their risk, making analyses such as that carried out in Sections 4.4–4.6 irrelevant to them. However, this does not mean that there are no security threats relevant to this group (or, indeed, risks to be reduced).

The least likely group of SSITUs to apply a RA process were families and individuals in their homes. None of our participants described any formal processes at home; their decisions were linked to their understanding of what security measures 'everybody' applies or to their workplace practices. Project participants linked to existing awareness initiatives aimed at SSITUs highlighted how their metrics for success showed more engagement from individual home users than from small businesses. These differences may be highlighting the difference between technology as a part of daily life and a business process — perhaps businesses need more justification to apply security measures, or perhaps they are suspicious of the motivations behind advice offered to them (this question is discussed in Section 6).

Our participants indicated that other SSITUs in need of some understanding of risk will, depending on their requirements, fall somewhere on a continuum between the activities of a large corporate entity and a home user.

Figure 7 expands on the contextual barriers described in Section 3 by illustrating the barriers SSITUs face in implementing the risk assessment process. When these difficulties combine, it shows why SSITUs in our study would struggle to implement any of the existing formal risk assessment processes — although some SME-specific standards, such as that of the aforementioned IASME, have a more adapted process.

Alongside risk, our dataset provided a number of other incentives SSITUs may have for implementing security. These are discussed in conjunction with risk in the following section.

5. THE ROLE OF RISK IN STRENGTHENING THE INCENTIVE FOR SSITUS TO SECURE

Our dataset has highlighted a number of types of incentives, other than the traditional identification of risk, for SSITUs to improve their security:

1. The protection of vulnerable users.
2. User vulnerability — awareness of a lack of knowledge.
3. The protection of privacy.
4. Cyber security fashions or due-diligence.
5. A regulatory or contractual requirement to report incidents.

These incentives will be relevant to different subgroups of SSITUs, depending on the formality of their IT processes, just as the risk assessment process is only applicable to a subset of SSITUs (as described in Section 4).

5.1. Incentives for individuals, families and informal groups

Incentive types 1–4 may explain the heightened uptake of security by home users (where SMEs have been slower on the uptake). Risk is less relevant to some SSITU subgroups, who are willing to follow basic guidelines in exchange for maintaining their confidence in the systems they use.

5.2. Incentives for small businesses, charities and clubs

Commercial (or at least more formalised) small organisations may need a more tangible reason to invest in security measures. Incentives 4 and 5 should provide greater incentives to businesses than incentives 1–3. Cialdini highlights the power of the message that *everybody else is doing something* when compared to other types of message [24]. In the case of cyber security this is likely to be defining what is considered basic due diligence — the use of antivirus, automated updates and regular backups. There is evidence of

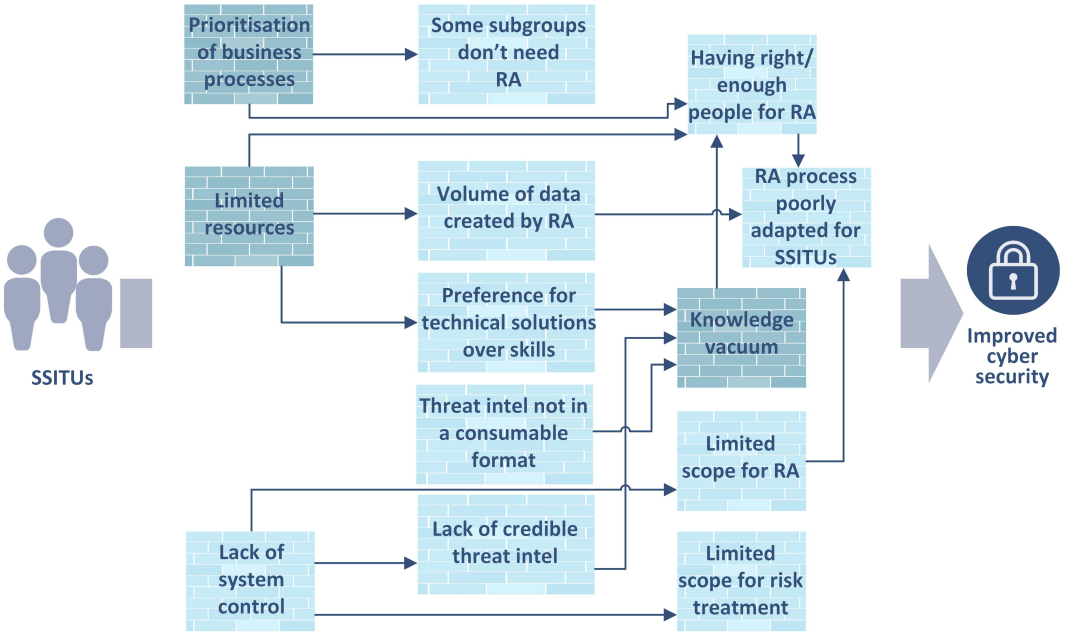


FIGURE 7. Contextual and procedural barriers to the implementation of cyber security

this in our dataset: the majority of participants choose to pay for antivirus without being able to explain either what the software does or its effectiveness on overall security. They, like individuals and families, will also have benefited (perhaps unthinkingly) from 'secure defaults' in operating systems, etc. Although our dataset includes information about SMEs using these default security measures and information about budgets, it does not differentiate between active choices made as a result of advice or fashion, or participants taking credit for using default settings.

These basic security measures have the advantage of fitting the criteria outlined by one SME owner — they are "cheap, fast and easy to deploy". A disadvantage is that they only protect against the most basic opportunistic attacks. Further, they highlight that many SSITUs' measure of due diligence is divorced from any measure of risk and there may be pockets of SSITUs who have no 'good' examples in their communities, leading them to identify a low benchmark.

With the increase in the number of organisations assuming that compromises are inevitable, incentive 5 may not be effective in isolation — its result may be a more accurate or higher calculation of the cost of a broadly defined risk of cyber incident. Our participants highlighted a number of examples of SMEs' questionable commitment to cyber security, with easy, fast and cheap mitigations being given priority over more impactful mitigations, a lack of investment in expert advice, and 'standard' (fashionable) security measures being perceived as 'good enough'.

5.3. An example of risk awareness changing incentives

Our dataset provided examples of how knowledge of security risks might increase other types of security incentive. For example, despite questionable commitment, "reputation is everything" to small organisations. As mentioned in Section 4.5, understanding cyber security risks is a key factor in their cyber security decision-making processes: even without the documented business processes of a larger organisation, smaller businesses in particular need to be able to measure risk. Their inability to correlate security risk with other business risk is contributing towards the former being taken less seriously.

As reputation is such a strong motivator, the ability of an organisation to limit impact once the risks of security breaches become more concrete should incentivise small organisations to develop reactive security processes. The Institute of Chartered Accountants in England and Wales (ICAEW) advise their members that a "bad response" to an incident is where the impact of a breach is amplified by a slow reaction and poor communication [13]. Good communication alongside the speed of detection and action was also felt by SSITUs to be crucial in surviving a breach. However, low knowledge leads to slow reactions.

One thing SMEs highlighted as a limitation in their ability to create an incident response plan was a lack of knowledge within the organisation. Our dataset did indicate that smaller organisations might lack the expertise needed to implement advanced security policies and measures. This implies that having low knowledge can increase the likelihood of mistakes.

Examples of successful attacks on companies in our study showed that employee mistakes contribute as much as malicious action. In one small participant company, (which did have a security function) employees were so embarrassed about being duped that they attempted DIY remediation before reporting the breach, reportedly increasing the impact of the attack.

Low resources and the ways in which money is spent is limiting the extent to which cyber security good practice and resilience measures can be implemented. Low knowledge is also a form of resource constraint, but decision makers' awareness of the increasing cost of mistakes may provide incentive for focusing more security investment towards human resources in small organisations.

The event chain described in this section — the identification of risk leading to the development of a business process that highlights a requirement for additional training in an organisation — indicates the importance of developing an accessible RA process to improve engagement in the commercially-minded subset of SSITU groups.

5.4. Where risk awareness does not increase security

Although we have shown that a more accessible form of RA than is currently available would be beneficial to some SSITUs, risk may not have the level of influence on security decisions that the other stakeholder groups — SPs and RHs — might hope for.

Our participants highlighted a number of reasons why their RA may not produce a higher level of security requirement:

- Their IT dependence outweighs cyber risks.
- Cash flow risks of investing in new equipment or services outweigh cyber risks.
- Their assets have a low value or are legally protected (copyright, etc.).
- The highest value assets aren't controlled by the SSITU (social media identities, etc.).

Figure 8 illustrates how the incentives and disincentives discussed in this section influence SSITUs' capacity for cyber decision making. As can be seen, although the disincentives provide a few additional barriers, the incentives provide a number of circumventions to the barriers illustrated in Figure 7, increasing the likelihood of a SSITU implementing some security.

However, a RA process will inevitably lead to decisions *proportionate to the risks faced by that organisation.* One of the complexities highlighted by our dataset is that the stakeholders most invested in improving SSITU security are not the SSITUs — the RH stakeholder group is attempting to measure SSITU security against their own risks, which is discussed in more detail in the following section.

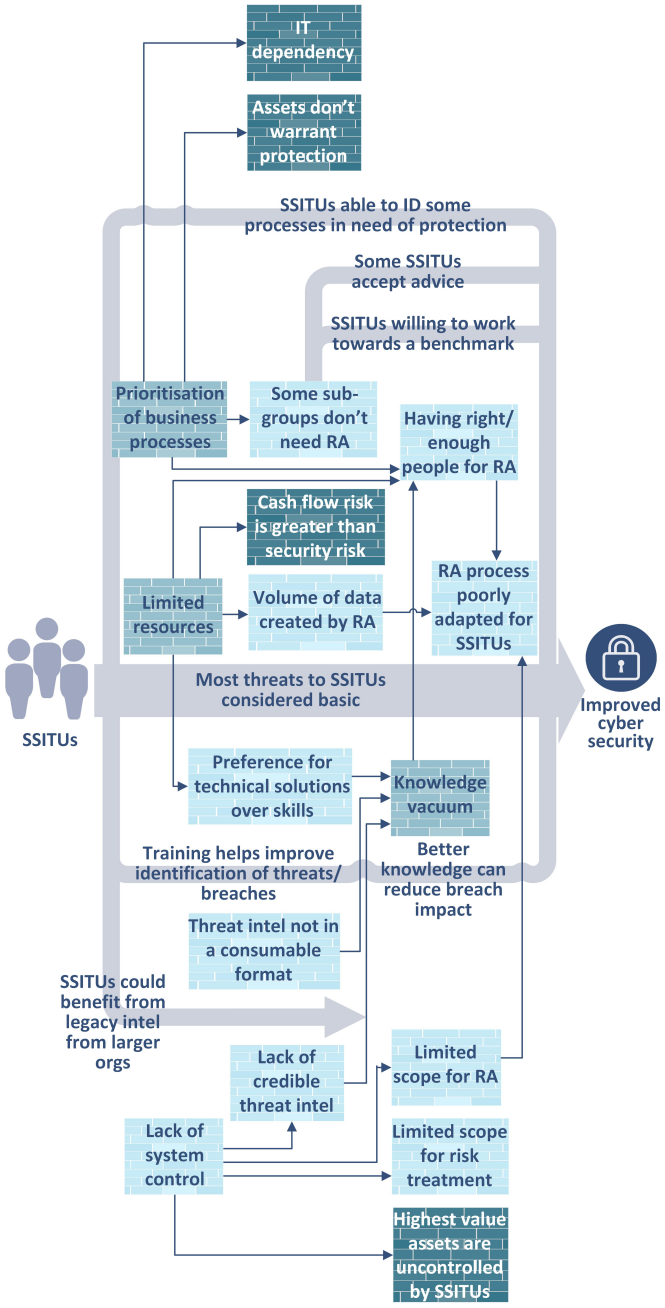


FIGURE 8. Incentives that circumvent barriers to the implementation of cyber security

6. SECURITY INCENTIVES AND DISINCENTIVES FOR RISK-HOLDING STAKEHOLDERS

The high level of interactions in the supply chain described in Section 4 leads to shared risks. This not only means that SSITUs are transferring risks to their service providers, but SSITUs are also becoming SPs to other SSITUs or larger organisations in the RH stakeholder group. This prompts a question about decisions in the supply chain: what happens when one organisation owns the infrastructure, another the data, and a third the risk? The concerns of the RH

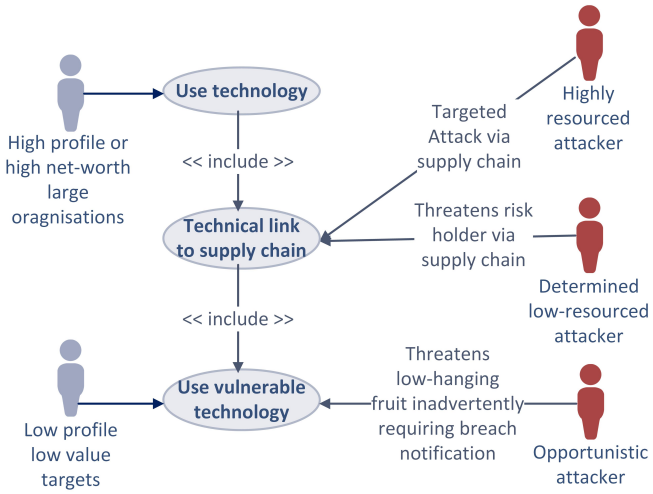


FIGURE 9. Misuse cases concerning the supply chain

stakeholder group are summarised by the misuse cases illustrated in Figure 9.

For the remainder of this section we will discuss the RH stakeholder group in our dataset: the reasons they have to be concerned about the security implemented by SSITUs; how they attempt to reduce this risk; and the result of these attempts to reduce risk on the overall small-scale cyber security dialogue.

6.1. Concerns about SSITUs' security from risk-holding stakeholders

In Section 4 we discussed how complexity in system control and ownership influences the decisions made by SSITUs, which, when combined with the level of concern our RH stakeholders described, might indicate that a certain amount of pressure (and so incentive to secure) is coming from the supply chain.

In fact only two of the SMEs who answered our questionnaire stated that they risked losing customers if they do not implement a cyber security standard. This could indicate that, although they are aware of the risk cyber security poses in their supply chain, few customers are currently attempting to influence their suppliers' cyber security decisions. In contrast, a KPMG survey suggested that 94% of procurement managers consider cyber security standards in the decisions they make when buying from SMEs[18] — suggesting either that the problem is being downplayed, or that the subset of SMEs interacting directly with large organisations may become more likely to engage with security practices. One participant highlights how the perception of standards may be the result of too many degrees of separation between the RH and the SP members of the supply chain: an SME may not have a direct contract with the RH, or may be depending on a third party to provide adequate security.

Our data indicates that securing reputation is becoming the most effective incentive for security. Although many organisations outsource IT, they fail to outsource cyber risk. However, the source of a risk is irrelevant — the reputational damage will be the same.

Organisations need the speed and efficiency of interconnected systems to be competitive [23]; they also wish to work with smaller suppliers who are more cost-effective. This forces them to accept a certain amount of risk, but also provides incentives to try and influence cyber security in the wider supply chain.

Some RH stakeholders mentioned extending standards down the supply chain as a means to ensure security, although, unlike quality management standards, participants indicated that the price of implementing the ISO cyber security standard makes it unattainable for most micro- and small companies.

One participant said that, rather than using standards as a benchmark, the standard of security expected from their supply chain was outlined in contracts. The contractors on-site also attended cyber security training. However, this participant also highlighted how subcontracting meant that security was not maintained at the standard they might have wished — the incentive to secure diminishes as the degrees of separation grow, along with the RH's ability to enforce security requirements.

The lack of ability to enforce security requirements down the supply chain has led to some RH stakeholders in our study becoming SPs to SSITUs. This is discussed in the following subsection.

6.2. Risk-holders as security-providers

In an attempt to manage their own risk, a number of RH stakeholders described how they had also become SPs to SSITUs. The best examples of this in our dataset are from government participants (advice as a risk-reduction measure) and a technology provider (product-embedded security as a reputational risk-reduction measure). While enforcing standards throughout the supply chain is proving challenging, other RHs may also be adopting this approach.

Our government participants report visibility of credible cyber security threats to SMEs. The risks that this poses to the stability of the UK, such as the economic risk of widespread attacks, prompted some inclusion of small organisations in the UK National Cyber Security strategy[19]. The strategy attempts to promote cyber security market growth, protection and awareness, which extends to SSITUs.

These three goals indicate that the risks identified by the UK government have incentivised the reduction of the number of constraints that limit both the

[18] www.cyberaware.gov.uk/sites/cyberstreetwise/files/cyber_streetwise_kpmg_-_small_business_reputation_report_final.pdf

[19] www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

implementation of security and the increase in cyber security suppliers for the sector.

The sheer numbers of small organisations who are potentially vulnerable makes individual support infeasible, but also makes pervasive small breaches a risk to the UK economy. This removes incentive to directly provide advice where an organisation is not part of the critical national infrastructure (CNI); however, methods of increasing awareness on a large scale are being developed in several initiatives (as already discussed).

One of the issues described by law enforcement participants is the need for SSITUs, despite the constraints they are under, to take responsibility for their own security as far as possible. While the authorities can provide some support, there is insufficient budget to deal with cyber breaches in large numbers, in the same way that there is insufficient police presence to ensure that houses without locked doors remain secure. Law enforcement needs to manage users' expectations and focus on educating the public — there is no mitigation against a victim's ongoing disinterest or lack of investment.

Holding responsibility for risk can in itself act as an incentive — the embarrassment of falling victim to an attack and an awareness that they (as uninsured RHs) would have to absorb the costs of any successful attack. Some people go as far as suggesting that suppliers such as banks used by SSITUs should be doing less to protect their customers, forcing them to take responsibility for their own risk[20].

The final incentive for government to assist small organisations with cyber security comes from the problem scope. International co-operation is needed to tackle pervasive commodity threats and intelligence helps to identify criminal networks. Both of these processes are out of the reach of SSITUs acting independently of government assistance.

In contrast to the attempts of the UK government to protect government assets, CNI and the economy, our technology provider needs to protect their reputation, indicating their acceptance that the impact of cyber breaches inevitably becomes shared across the supply chain.

Van Eeten and Bauer [17] suggest that the incentive for suppliers to take responsibility for security due to the need to protect their reputation is growing: their income is reliant on customer trust, and SSITUs in our study expect and assume products are secure. It is important for suppliers to provide continuity/stability of service and devices that function, as they are the first people a user is likely to contact when a problem occurs.

IT-driven business models create ongoing relationships between customers and suppliers [23] — an ongoing demonstration of good quality products becomes an incentive to invest in security. Perceived insecurity becomes damaging to product vendors — a good example of this is the preference of several security aware participants *not* to use Microsoft Windows for security reasons. This damaging reputation does not necessarily reflect the quality of the product, just the level of awareness users have of its vulnerabilities.

Customers represent a reputational risk to suppliers if they are insecure — some participants stated that they considered avoiding risky suppliers *and risky customers* to be good cyber security practice. In the case of customers demonstrating poor cyber security practices, the risk is not only reputational — shared hosting, etc. could put other customers at risk. In these circumstances it is understandable that RH stakeholders first attempt to become SPs, before choosing to withdraw services from those exhibiting poor security practices or the high risk described in Section 4.6.

The technology provider would have success improving security by adapting their own products; however, the provision of advice from RH stakeholders has mixed success. Our dataset indicates that the group of SSITUs we defined in Section 3 as not requiring a risk assessment have been more receptive to advice than the group with more formal business processes. This is illustrated in an update of the overview of the barriers to cyber security we have presented a number of times throughout this paper (Figure 10). In the case of SMEs, the increase in advice provided by RH stakeholders has had implications on the level of credibility that advice is given, as discussed in the following subsection.

6.3. Trust from SSITUs

There is a risk, in certain circumstances, to a RH also becoming a SP, especially where security is provided in the form of advice.

Where the SME participants in our study were concerned, the lack of accessible evidence of a serious risk to the participants mentioned in Section 4, combined with the way cyber security is being presented by the other small-scale cyber security stakeholders, may highlight how the needs and motivations of non-SSITU stakeholders might influence the decisions made by SSITUs.

In the example of the government as a SP in the previous section, the fact that the threats visible to those developing the advice is not visible to SSITU decision makers may be reducing their trust, irrespective of any intention to study the evidence.

The following participant statements are other examples in the dataset of a lack of trust in sources of information or support in implementing cyber security:

- "Knowing where to turn for up to date accurate unbiased information."
- "Lack of a single source of information. Inability to know the standard/quality of information we find

[20] www.theguardian.com/uk-news/2016/mar/24/dont-refund-online-victims-met-chief-tells-banks

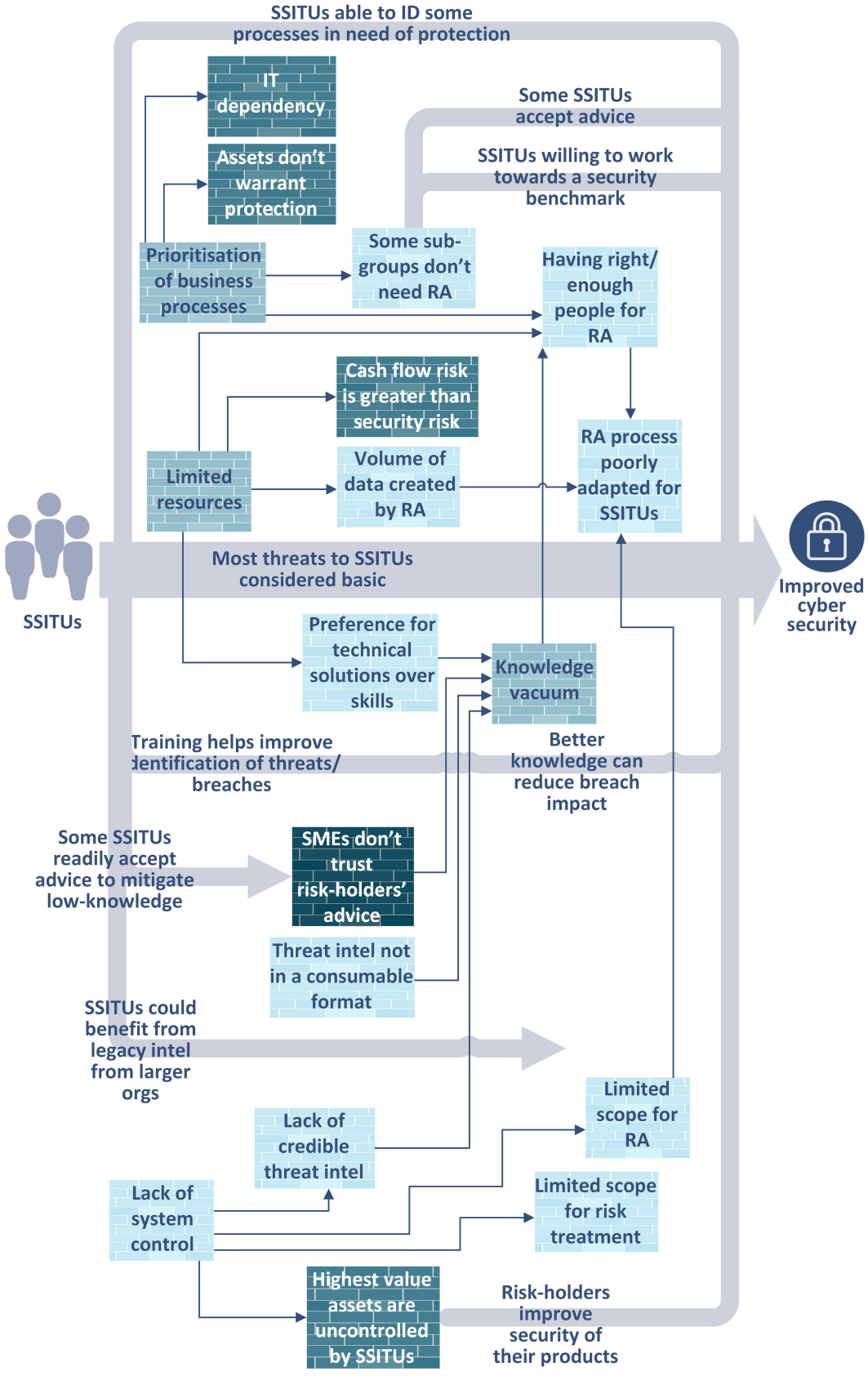


FIGURE 10. A final overview of the barriers to cyber security decision making, including the impact of RH stakeholders

on the internet. Scare stories"
- "The ability to get trusted expert advice. I know enough about cyber security to know that, you need to be a real expert, a lot of the businesses touting cyber security 'expertise' to SMEs have no in-depth security expertise and are just jumping on the band wagon."

These varying expressions of a lack of trust in the quality of available information and assistance illustrate why the dialogue between different members of the SME cyber security ecosystem is so disjointed. A growth in the number of new initiatives focused on SMEs, aiming to supply basic information, could be an indicator that government and large industry are interpreting the lack of interaction as a sign of inaction.

The reality of the situation may be slightly different. The majority of the SSITU participants are suggesting that they are not sure where they stand where cyber security is concerned. The indication is that, despite this, all the respondents — even if they openly admit they do not care what cyber security is — are attempting to understand the risk they face or existing security benchmarks, and, as a result, are implementing some form of cyber security measures.

In addition to the consistency of advice advocated by Renaud [14], an increase in transparency from the risk-holding SPs about the threats they have detected may be needed for their initiatives to succeed. There is also the question of advice relevance as RHs and legislative requirements evolve: as the UK government begins to hone its advice to focus on the prescriptive measures in the aforementioned Cyber Essentials scheme, the new General Data Protection Regulation[21] will require SSITUs to carry out privacy impact assessments on specific data they hold, requiring records of a cyber security decision-making process. Cyber Essentials will undoubtedly increase the security of a high proportion of SSITUs, but when (after reputational damage) the most recognised risk is in failing to protect client data, advice may need to adapt to show how to link essential security measures to specific datasets.

A change of perspective in the supply chain may also be required: while smaller organisations are traditionally risk-takers — unable to greatly influence suppliers or customers [10] — in the case of their ability to influence cyber security, the asymmetry between large and small organisations seems to be reduced. An attacker only needs one point of entry to a system: the size of the door isn't necessarily relevant to the impact of the breach, meaning that closer partnerships are required to improve supply chain security.

7. CONCLUSIONS AND FUTURE WORK

Throughout this paper we have evaluated the ways in which our survey has highlighted the differences between small-scale IT users (SSITUs) and larger government or corporate entities with regards to the technology they employ and its impact on cyber security decision making. We have illustrated the difficulties and constraints a SSITU faces in justifying the implementation of security. Namely that:

- SSITUs are focusing on easy-to-implement technical measures, leading to a disconnect between the security implemented and any risks identified.
- Characteristics of SSITUs such as limited resources, knowledge and a need to carry out certain processes limit security decisions.
- Limitations in system control, available threat intelligence and the relevant employees make existing RA processes challenging, and make their outcomes less meaningful.
- Very few SSITUs face more than basic threats or employ more than basic security measures, unlike their neighbours in the supply chain.
- Assessing risk in SSITUs will not lead to sufficient investment to mitigate risks in our RH stakeholder group — the supply chain needs better collaborative processes to reduce their risk as a whole.
- RH stakeholders becoming security suppliers to SSITUs with limited dialogue are undermining SSITUs' trust of the security advice they are offered.

In introducing this paper, we posed the question *how do the constraints of a small organisation influence their risk perception and how they justify security investment?* We can conclude that the constraints faced by SSITUs have far more impact on the decisions they make than either our RH or SP participants may have anticipated. Any limitations faced by SSITUs as they make their security decisions will have a huge impact on both the measures they are able to apply and the security of the supply chain as a whole.

The datasets used in this evaluation have provided some useful data points to challenge some of the common assumptions made by cyber security experts. The selection of participants through theoretical (rather than random) sampling provided comparative information from within the small-scale cyber security ecosystem.The qualitative methodology used in this project does not specify a definitive measure of validity; rather, the success criterion of a Grounded Theory project is typically the extent to which the result fits with the data used to generate it [9]. In the context of this study, although some results are novel to the cyber security community, the SSITU participants to whom we released preliminary results felt that they accurately represented their position.

We intend to build upon these results. First, we will evaluate the reciprocal subject of system and cyber security architectures, providing information on how, once SSITUs justify any investments in cyber

[21] `http://www.eugdpr.org/`

security, the implementation of best practices may still hinge on the constraints faced by SSITUs. We will then draw from these analyses to provide a set of attributes of SSITUs for a requirements framework, highlighting constraints and global requirements for this user group, which could facilitate product development in this sector. Further research into the influence SSITUs have on the overall supply chain would also be valuable, providing information on how large RH stakeholders might best use their resources to influence SSITU security.

Acknowledgements

The authors would like to thank the reviewers for their constructive comments. Emma Osborn's research is funded by EPSRC via the Centre for Doctoral Training in Cyber Security at the University of Oxford.

REFERENCES

[1] Carroll, J. (1996) *Computer Security*, 3rd edition. Butterworth-Heinemann, Newton, MA.

[2] Pfleeger, C. P. and Pfleeger, S. L. (2007) *Security in Computing*, 4th edition. Prentice Hall, Boston, MA.

[3] Osborn, E. C., Creese, S., and Upton, D. (2015) Business versus technology: Sources of the perceived lack of cyber security in SMEs. *Proceedings of the 1st International Conference on Cyber Security for Sustainable Society*.

[4] Osborn, E. C. and Simpson, A. C. (2015) Small-scale cyber security. *Proceedings of the 2nd International IEEE CSCloud Conference*, pp. 247–252. IEEE.

[5] McGregor, S., Charters, P., Holliday, T., and Roesner, F. (2015) Investigating the computer security practices and needs of journalists. *In Proceedings of the 24th USENIX Security Symposium*, pp. 399–414.

[6] Ahrend, J. M., Jirotka, M., and Jones, K. (2016) On the collaborative practices of cyber threat intelligence analysts to develop and utilize tacit threat and defence knowledge. *In Proceedings of the 2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)*, pp. 1–10.

[7] Charmaz, K. (2014) *Constructing Grounded Theory*, 2nd edition. Sage.

[8] Guest, G., Bunce, A., and Johnson, L. (2006) How many interviews are enough? An experiment with data saturation and variability. *Field Methods*, **18**, 59–82.

[9] Corbin, J. and Strauss, A. (2008) *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage, Los Angeles.

[10] Wynarczyk, P., Watson, R., Storey, D., Short, H., and Keasey, K. (1993) *The Managerial Labour Market in Small and Medium-Sized Enterprises*. Routledge, London.

[11] Lee, G. and Xia, W. (2006) Organizational size and it innovation adoption: A meta-analysis. *Information & Management*, **43**, 975–985.

[12] Blau, P. M. (1970) A formal theory of differentiation in organizations. *American Sociological Review*, **35**, 201—218.

[13] ICAEW (2015) *Audit Insights: Cyber Security 2015*. ICEAW, London, UK.

[14] Renaud, K. (2016) How smaller businesses struggle with security advice. *Computer Fraud & Security*, **2016**, 10–18.

[15] Lazear, E. P. Entrepreneurship. *Journal of Labor Economics*, **23**, 649–680.

[16] Rhee, H.-S., Kim, C., and Ryu, Y. U. (2009) Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, **28**, 816–826.

[17] Van Eeten, M. and Bauer, J. M. (2009) Emerging threats to internet security: Incentives, externalities and policy implications. *Journal of Contingencies and Crisis Management*, **17**, 221–232.

[18] Dang-Pham, D. and Pittayachawan, S. (2014) Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A protection motivation theory approach. *Computers and Security*, **48**, 281–297.

[19] Subashini, S. and Kavitha, V. (2011) A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, **34**, 1–11.

[20] Caralli, R. A., Stevens, J. F., Young, L. R., and Wilson, W. R. (2007) Introducing OCTAVE Allegro: Improving the information security risk assessment process. Technical Report CMU/SEI-2007-TR-012. Software Engineering Institute, Carnegie Mellon University.

[21] Alberts, C. and Dorofee, A. (2003) *Managing Information Security Risks: The OCTAVE Approach*. Addison Wesley, Boston, MA.

[22] Gordon, A. (2015) *The official ISC2 guide to the CISSP CBK*. Taylor Francis, Boca Raton, FL.

[23] Kagermann, H., Osterle, H., and Jordan, J. M. (2010) *IT-driven Business Models: Global Case Studies in Transformation*. Wiley.

[24] Cialdini, R. B. (2003) Crafting normative messages to protect the environment. *Current Directions in Psychological Science*, **12**, 105–109.

[25] Li, F., Lai, A., and Ddl, D. (2011) Evidence of Advanced Persistent Threat: A case study of malware for political espionage. *Proceedings of 6th International Conference on Malicious and Unwanted Software (MALWARE)*. IEEE.

[26] Scott-Railton, J. (2016) Security for the high-risk user: Separate and unequal. *IEEE Security and Privacy*, **14**, 79–87.

[27] Lusthaus, J. (2013) How organised is organised cybercrime? *Global Crime*, **14**, 52–60.