SMALL-SCALE CYBER SECURITY

Mapping security requirements for IT users at home and in small organisations

EMMA OSBORN

A thesis submitted for the degree of Doctor of Philosophy

University of Oxford
Department of Computer Science and
Centre for Doctoral Training in Cyber Security

Trinity Term 2018

ABSTRACT

Despite a long-standing assumption that developments in personal and cloud computing models would change the way we approach security, small-scale IT users (SSITUs) remain underserviced by existent cyber security models. This dissertation discusses survey results relating to the technology employed by SSITUs and their engagement with cyber security.

We determine that: SSITUs are focusing on easy-to-implement technical measures, leading to a disconnect between the security implemented and any risks identified; few SSITUs face more than basic threats or employ more than basic security measures; 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 also found that: the system architectures employed by SSITUs are significantly different to those employed by large corporate or government entities; the architecture of a small organisation's digital footprint has far more impact on their overall security than would be the case for a large organisation; and SSITUs do not hold sufficient influence within the supply chain to manage cyber security in their interactions with service providers.

We show that improving small-scale cyber security architectures is not simply about developing new technology — there is a need to consider technology use in context of interactions within a broader ecosystem of a supply chain, users with multiple roles and conflicts of interest, as well as the increased importance of SSITUs' digital footprints on their security.

In order to improve the cyber security posture of the smallest organisations, security providers need a better understanding of their requirements and the role of larger stakeholders within the supply chain. They also need a business case for investing in products for this marketplace. To this end we have developed a framework of global requirements and constraints for small-scale cyber security, which should have the potential to assist in the development of products adapted for this user group.

For contrast we have provided a requirements framework developed from the perspective of the risk-holding stakeholders in the supply chain, to illustrate the differing expectations of the best-resourced stakeholders in their interactions with SSITUs. This highlights the difficulties posed by incumbent best practices, where many security measures are beyond the grasp of SSITUs and the risks some stakeholders expect to be reduced far exceed the means of the smaller organisations.

We conclude that, with a better understanding of the context within which SSITUs operate, combined with a suitable expectation of how much risk can be transferred to them within the supply chain, it is possible to improve small-scale cyber security.

ACKNOWLEDGEMENTS

EPSRC
Engineering and Physical Sciences Research Council

This research was funded by EPSRC via the Centre for Doctoral Training in Cyber Security at the University of Oxford.

With thanks to (in more-or-less chronological order):

Marc, who put me on the path to becoming a computer scientist, and the friends and lecturers who kept me sane while I was on that path... vous savez qui vous êtes.

Dr Kevin Jones, who convinced me to try this research thing.

My family, who didn't (audibly) sigh when I told them I was going back to uni (again).

The friends who offered love, support, boardgames, wisdom and the odd motivational speech when procrastination was getting the better of me.

David and Maureen — I always leave your office smiling.

Professor Sadie Creese, for her insight during the CDT mini-projects and the Late Professor David Upton, the only person I've ever met who could answer questions faster than I could ask them.

My project participants — thank you for both your time and your ongoing interest. This wouldn't have been possible without you.

And finally, Dr Andrew Simpson. Thank you for always being there, for always knowing what to advise and for always saving some time for your students.

...if you ignore the rules people will,
half the time, quietly rewrite them
so that they don't apply to you.

— Terry Pratchett, Equal Rites
(and SMEs on cyber security)

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

1.1 MOTIVATION

Technology is used pervasively by individuals, families and small organisations. In the UK, the motivation for including small to medium-sized enterprises (SMEs) in a national strategy is that: they currently account for 99.9% of UK private sector businesses, 60% of private sector employment and 47% of private sector turnover (figures that have been increasing since the year 2000) [28]; 88% of charities in the UK (approximately 145,000) are also classed as micro, small or medium by the UK Charity Commission [105]; and the privately run clubs and other less formal organisations all face similar security challenges to those of small businesses. Despite this, neither individuals nor small organisations typically spring to mind when one considers the term *cyber security*.

The impact on cyber security of the widespread adoption of ICT by small organisations is by no means a new phenomenon. Two decades ago Carroll [22] 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." [22]

As early as 1996, with the rapid growth of personal computing, people were differentiating the actions and requirements of small companies 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 highlighted over a long period of time, as well as by authors recognising the impact of moving to a more distributed computing model (for example, the first edition of Carroll's book was written in the era of the mainframe, so he highlights the differences personal computing brings to the question of security in later editions [22]), the question of the different security requirements faced by smaller organisations has, unfortunately, been left largely unresolved.

The UK Government released National Cyber Security Strategies in 2011 [109] and again in 2016 [115]. Both mention enhancing the security of consumers and smaller organisations as part of a broader aim to support economic growth. However, neither the aims described in the 2016 strategy nor contributions to the academic literature demonstrate that significant progress has been made in securing these smaller-scale IT users against cyber threats since 2011.

The majority of government cyber security funding (98%) was allocated to securing government departments and critical national infrastructure against 'high-end' threats and developing a national capability — it was, after all, a risk-based prioritisation of activities. However, one reason for highlighting this division of funds is to highlight an endemic problem: if large organisations with large network infrastructures are the main consumers of cyber security products and services then it is unsurprising that security researchers continue to focus on developing tools for this sector and professionals continue to be trained using examples of large IT systems.

Widely publicised attacks tend to have microscopic focus, concerning themselves with a single technical aspect of a system, e.g., Windows Server Message Block Protocol in the case of WannaCry (CVE-2017-0144[1]), Bash in the case of Shellshock (CVE-2014-6271; CVE-2014-7169) and OpenSSL in the case of Heartbleed (CVE-2014-0160). Security risks tend to be mitigated by cyber security products that consider specific aspects of system architecture, from web browser add-ons to placing data diodes in a network. However, when security is considered at a macroscopic level, it becomes clear that small and large entities are not working with the same IT models and there are issues scaling either type of system to suit a differently sized organisation.

While the cyber security industry (understandably) focuses on protecting the high value assets typically owned by organisations able to, either directly or indirectly, fund research and development, the use of programmable systems by individuals, families and small organisations is ubiquitous.

In [80] Pfleeger and Pfleeger highlight how the ubiquity of computing has saddled users with a responsibility for security that they have neither the awareness nor the motivation to handle — leading to a mismatch between security measures and risks. This pattern is repeated in the UK's 2016 report on the National Cyber Security Strategy, which stated that smaller businesses' *"awareness of the personal relevance of the cyber risk is patchy"* [116].

Internet penetration far outstrips employment rates in developed countries, which tend to be less than 60% of the population above the age of 15[2]. If we consider the UK, around 60% of employment is provided by Small or Medium-sized Enterprises (SMEs). This means that, in addition to the technological aspects of cyber security models lacking downward scalability, the proportion of UK residents who are likely to have experienced the training aspects of corporate-style cyber security models is relatively low. Numerous communities are left without access to examples of 'good' cyber security practices against which to benchmark their own activities.

Taken together, these and other factors give rise to a large group of internet users who have limited resources in terms of finance, time and knowledge, and for whom the traditional cyber security marketplace is ill-adapted. They are a group of individuals, who, whatever their roles, do not have the benefit of cyber security training and support often offered by a large employer. We refer to this user group, whose use of technology does not fit the prevailing corporate cyber security model, as *small-scale IT users* (SSITUs — defined in Chapter 2, alongside the two other small-scale cyber security stakeholder groups: risk-holding stakeholders and security providers).

1 CVEs referenced from the Common Vulnerabilities and Exposures Catalogue held at cve.mitre.org/cve/cve.html

2 The World Bank working age employment to population ratio (2015): data.worldbank.org

We describe how downward scalability and appropriate cyber security measures are increasingly important, due to increasing system interconnectivity meaning that large organisations are finding it harder to isolate themselves from smaller entities. As security measures improve within the highest value cyber targets, attackers find they have more to gain from exploiting easily accessible vulnerabilities within the smaller, less well-protected organisations, from which they can also gain a foothold in a trusted system to attack their original target. Currently, the financial implications of carrying this risk are not being passed down the supply chain to the smaller user, which does not help encourage adoption of cyber security measures [76]. However, the question also has to be asked: how accessible are suitable cyber security measures to small companies with limited resources and little by way of company-owned network infrastructure?

The rationale behind this research was to provide information about the landscape of the small-scale cyber security ecosystem, allowing stakeholders to refine their attempts at engaging SSITUs in cyber security. Our definition of a small-scale cyber security requirements framework is intended to begin structuring the cyber security needs of SSITUs, as well as highlighting the conflict in requirements from their supply chain. It highlights how much the SSITU cyber security landscape is influenced by external pressures, which may have limited the success of past initiatives. While we do not promise that these conflicting requirements frameworks provide a simple answer for those hoping to access a largely untapped marketplace, it does align the problem of securing SSITUs with Rittel and Webber's definition of a "Wicked Problem" [88], explaining why some reductionist scientific approaches may need to be based upon a broader description of the problem landscape.

1.2 RESEARCH QUESTIONS

The work reported on in this dissertation focuses on the question:

> *If existing large corporate cyber security and governance practices are not well adapted for small organisations, how might we enumerate and articulate small-scale IT user requirements for security?*

The work undertaken was informed by the following questions:

1. *Who are the members of the small-scale cyber security ecosystem?*
2. *How do the constraints of a small organisation influence their risk perception and how they justify security investment?*
3. *Once a SSITU has justified investing in cyber security, what constraints within their IT system limit their decisions?*
4. *How can understanding the context that SSITUs operate within assist in the development of a small-scale cyber security requirements framework?*

1.3 CONTRIBUTIONS

The dissertation presents three contributions, namely:

1. A survey of the context in which SSITUs make decisions about cyber security, the barriers they may face in implementing a risk assessment, and understanding threats and how this contrasts with the expectations of risk-holding stakeholders in the supply chain.
2. A survey of the architectures, digital footprints and inter-system interactions employed in SSITUs' IT systems, highlighting the constraints of mitigating risks within a complex partially-controlled system (these two contributions answer the questions posed in research questions 2 and 3).
3. A requirements framework that uses the attributes of SSITUs described in the preceding two contributions to provide information about small-scale cyber security to any organisation attempting to develop products for the sector, answering research question 4.

1.4 PAPERS ARISING FROM THIS WORK

The work described in this dissertation has contributed to a number of papers, either published or submitted for publication:

- Contributions from introductory chapters:
  1. Small-scale cyber security.
     Emma Osborn and Andrew Simpson.
     In Proceedings of the 2nd International IEEE CSCloud Conference, pages 247–252. IEEE, Nov 2015 [71].

- Contributions from our UK case study on SSITUs (Chapters 4 & 5):
  2. Risk and the Small-Scale Cyber Security Decision Making Dialogue — a UK Case Study.
     Emma Osborn and Andrew Simpson.
     Accepted by The Computer Journal, Apr 2017 [75].
  3. On Small-Scale IT Users' System Architectures and Cyber Security: A UK Case Study.
     Emma Osborn and Andrew Simpson.
     Computers and Security, 70:27–50, Sep 2017 [73].
  4. On safety and security requirements in emerging ubiquitous computing models.
     Emma Osborn and Andrew Simpson.
     The Computer Journal, 59(4):570–591, Jan 2016 [72].
  5. Business versus technology: Sources of the perceived lack of cyber security in SMEs.
     Emma Osborn, Sadie Creese, and David Upton.
     In Proceedings of the 1st International Conference on Cyber Security for Sustainable Society, Feb 2015 [76].

- Contributions from Chapter 6 — defining a small-scale cyber security requirements framework:

    6. A Requirements Framework for Small-Scale Cyber Security.
    Emma Osborn and Andrew Simpson.
    In preparation, Oct 2017 [74].

1.5 DISSERTATION STRUCTURE

The dissertation structure reflects the questions outlined in Section 1.2: Figure 1 illustrates the link between research questions, the dissertation structure and the papers that have arisen from this work.

Chapter 2 outlines the SSITU group and other small-scale security stakeholders (answering research question 1), followed by a broad literature review. Chapter 3 then outlines the research approach. Chapters 4–6 represent the three contributions of this dissertation: Chapters 4 & 5 describe the the small-scale cyber security landscape provided by our analysis of participants' insights; Chapter 6 makes use of this knowledge to elicit requirements and demonstrate the difference in perspectives of the stakeholder groups.

As well as focusing the project on eliciting the cyber security needs of SSITUs, the project design was heavily influenced by the constraints SSITUs face in interacting with research. A reflection on the presented findings, as well as the methods used to gain access to the SSITU group, can be found in Chapter 7, where we draw conclusions.

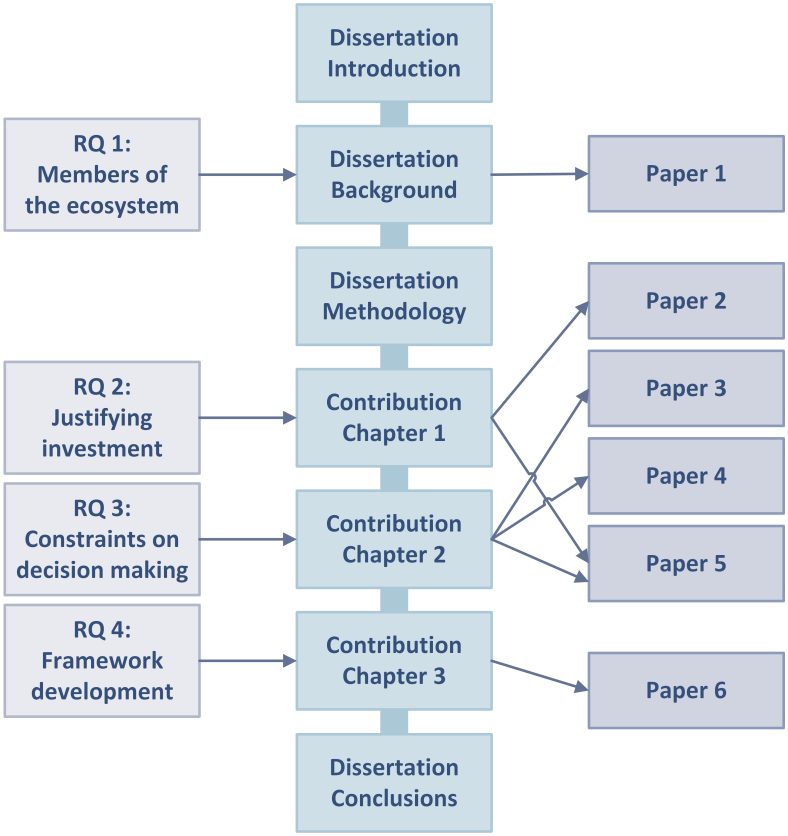


Figure 1: *An illustration of the relationship between research questions, dissertation structure and papers*

2

BACKGROUND

In introducing this dissertation we described how, in the development of incumbent cyber security practices, solutions were better-adapted to the needs of larger organisations. This chapter begins by defining stakeholder groups in the small-scale cyber security ecosystem, including the small-scale IT user (SSITU) group, whose operational needs may be incompatible with existing cyber security practices.

The small-scale cyber security ecosystem is incredibly complex, with SSITUs interacting with each other, their supply chains and the cyber security industry in many different ways. Figure 2 highlights some key areas where the incumbent large-scale cyber security, safety and privacy practices intersect with SSITU cyber security practices, using as boundaries the phenomena that arose from the analysis presented in Chapters 4 & 5.

Due to this complexity, once the stakeholders of the small-scale cyber security ecosystem have been defined, we provide a comprehensive literature survey, split into five sections. These explore both existing knowledge of SSITUs' interactions with cyber security and the intersections between small-scale cyber security and the incumbent practices of Figure 2. Figure 2 also highlights the diversity of sources from which we have had to draw this literature survey — cyber security for this user group is so under-researched that there is no coherent canon of literature.

Section 2.2 discusses the representation of the various SSITU groups in publications, as well as related subjects such as descriptions of their general IT use and business processes. Section 2.3 then provides insight into the business models that underpin the provision of IT to customers small enough to be considered 'consumers'. Sections 2.4 to 2.6 then describe practices that may influence or constrain SSITU use and common but inaccessible practices. We have attempted to include sufficient examples from each existing practice to describe the knowledge gap, although the dispersion of literature across so many subject areas made an exhaustive survey impossible. In some cases, articles from non-academic sources have been included to discuss the information presently available to SSITUs, although these sources often do not provide sufficient detail about their methods for us not to question their findings.

Section 2.7 summarises the chapter.

2.1 DEFINING SMALL-SCALE CYBER SECURITY STAKEHOLDERS

As discussed in Chapter 1, the first research question we address is *who are the members of the small-scale cyber security ecosystem?* As a result of an initial study in [76] we presented the results of a survey of SMEs' perspectives on cyber security issues and described the often disjointed dialogue between the stakeholders in this ecosystem. The study identified three primary stakeholder groups in the SME cyber security ecosystem: the SME IT user group; those supplying cyber security measures to this user group; and those concerned about the implementation of cyber security in SMEs.

In this dissertation, we expand this user group to consider all small-scale IT users (SSITUs).

Building upon this initial study we define the small-scale cyber security ecosystem as three stakeholder groups:

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)).

Thus far, SSITUs have been defined by *what they are not*: they are not entities with sufficient resources, infrastructure or requirements to warrant deploying (often expensive) existing corporate cyber security practices. This includes small to medium-sized enterprises, startup companies, volunteer-run organisations such as small charities or private clubs, families and individuals who do not have the benefit of cyber security training from a large organisation. Figure 3 illustrates the user groups where there are no individuals who have benefited from observing or learning from the mature cyber security practices of a large organisation. In some groups — families, for example — other individuals who benefit from being embedded in larger organisations may provide this knowledge. In other groups there may be less diffusion of skills, for example, to businesses or charities from interactions with larger collaborators.

By defining a user group whom it does not fit, this definition supports our argument that current cyber security practices are not inclusive. However, this does not mean that SSITUs form a single user group with a coherent requirements set.

It is also worth highlighting that none of the user groups, including the corporate IT users, are mutually exclusive. This is also illustrated in Figure 3, which illustrates where user groups may overlap. The majority of corporate and small organisation IT users will also be home IT users — as both individuals and families, as susceptible to cyber security risks specific to an individual as those IT users with no affiliations. The difference between the user groups will be blurred, depending on the proportion of users residing in the intersections between groups. This blurring between user groups may not be seen to obviously impact on technology choices or cyber security risk in a particular location, but it is likely to increase the number of use cases for connecting to the Internet in a given environment, and will clearly impact upon the knowledge and attitudes towards cyber security that users bring into the environment.

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.

These definitions can be used as a starting point, to begin describing the small-scale cyber security ecosystem. However, the way in which they employ business processes and IT systems described in Chapters 4 and 5 will provide additional parameters.

2.1.1 *SMEs*

SMEs may be new or mature businesses — with startups being a subset within this group — with size having a significant influence on how they operate in terms of

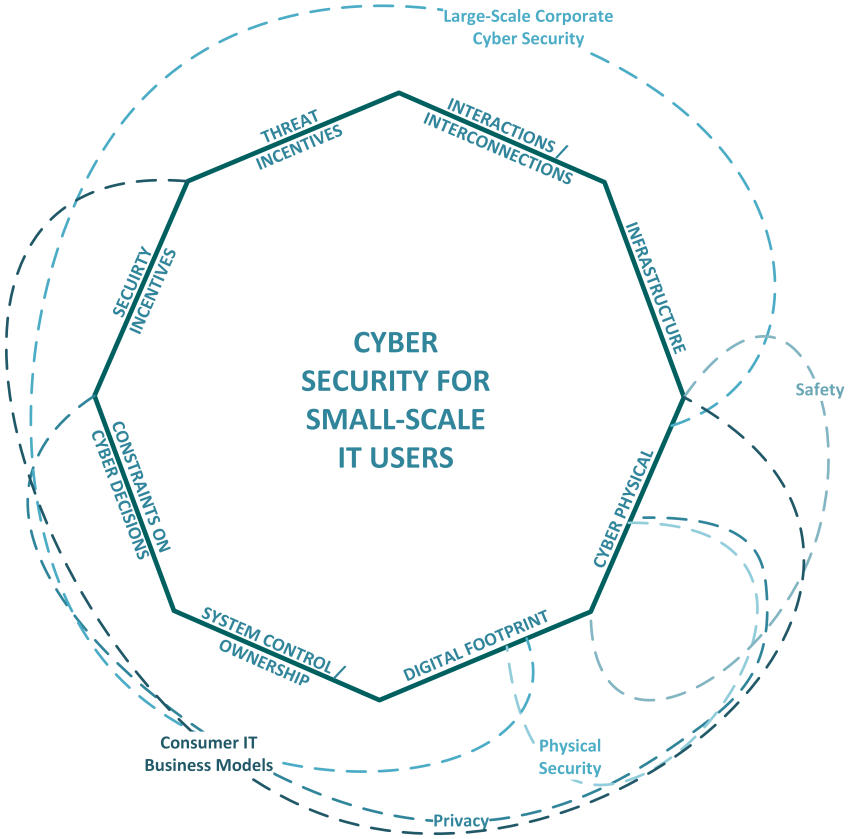


Figure 2: *High-level illustration of small-scale cyber security's intersection with existing practices*

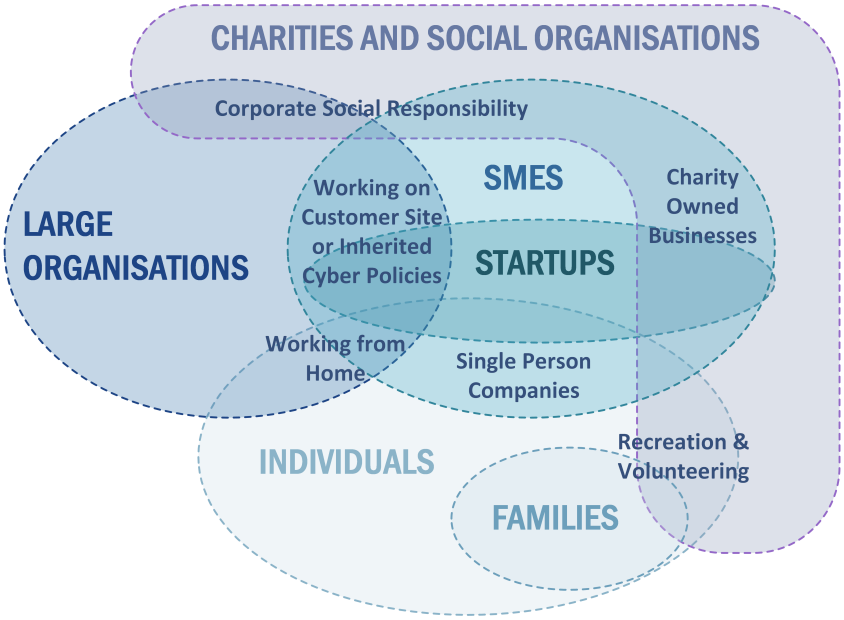


Figure 3: *An illustration of the overlaps between different user groups, used to highlight the lack of penetration of large organisations' knowledge into certain groups*

Company Type	Employees	Turnover / Balance Sheet
Medium-sized	<250	⩽ €50m or ⩽ €43m
Small	<50	⩽ €10m or ⩽ €10m
Micro	<10	⩽ €2m or ⩽ €2m

Table 1: *EU SME definition [32]*

business processes, strategy and company culture. The European Commission states that 99% of businesses in Europe are SMEs, using the definition provided in EU law (EU recommendation 2003/361 [32]), as outlined in Table 1.[1]

Startups differ from SMEs in that they typically operate at extremely high risk in order to facilitate rapid growth. There is a chance that the owner's exit strategy and company saleability could play a greater role in how a startup considers cyber security than would be the case for a typical SME.

2.1.2 *Charities and private clubs*

There are organisations of a comparable size to SMEs that are not run as businesses. We identify two other groups here: charities and private clubs.

Charities are heavily regulated organisations existing for charitable purposes (which the UK defines directly in legislation, employing the Charities Commission to oversee the running of charities [108]). As described in Chapter 1 the Charities Commission also classifies charities according to their size, with 88% considered to be micro, small or medium-sized. Despite this heavy regulation, unlike small businesses, small charities will still operate with volunteers — often even at board level.

We consider private clubs to be small, informal social organisations that have a cyber footprint with which their members are associated, although the level of formality applied to other processes — if they exist only as an online community, whether they are committee-led, if they have an address, bank account or membership fees, etc. — can vary. Some of these organisations are defined in UK law for the purposes of equality, licensing and revenue and customs. For example, the Equalities Act describes *private clubs and other associations* as organisations of 25 or more members, with club rules, that are neither trade organisations, nor openly accessible to the general public [106].

Charities and private clubs can be of a comparable size to SMEs and startups, but they exist for very different reasons. This is reflected in their culture and the decisions they make, which will influence how they use technology. Their IT use may be of a similar scale, but the products and policies they choose will be influenced by the interests and skills of their volunteers.

1 It should be noted, however, that this definition is not universal — in many countries, including the USA [117], the threshold below which a company is considered a small to medium-sized enterprise or business (SME or SMB) is 500 employees, rather than 250.

2.1.3 *Individuals and families*

Considering an individual as an IT user separately from their work status and the other user groups of which they are members is significant in terms of their motivation for using devices and services. This is important in how users construct their privacy requirements and their overlap with cyber security at an individual level.

Each individual IT user has their own digital footprint, as well as having contributed to the digital footprint of whichever organisations they are associated with. Individuals' motivations for using technology at home will be different from those they have at work, and they may adapt the decisions they make and the risks they are willing to take accordingly [27].

As well as the digital footprint associated with an individual, many people will have an associated (but not identical) digital footprint for their family or household. This can include shared infrastructure, shared online services, a nominated technical expert, and shared decision-making to protect vulnerable members of the group. This shared digital footprint may not be reflected in the material world, but it is distinct from the digital footprint of an individual.

For the purposes of scoping in the project design described in Chapter 3, the assumption has been made that individuals embedded in large organisations will have been influenced in their cyber security practices. In most cases we will handle this by taking about the SSITU group, where a total lack of access to corporate knowledge of cyber security heavily influences the capacity to implement cyber security. In other instances (in Chapter 5's discussion of different roles in the digital footprint, for example) we loosen this definition to discuss risk-holding stakeholder concerns about the conflicts of interest faced by people in multiple user groups, which brings their employees back into the SSITU user group.

2.1.4 *Risk holders*

The risk-holding stakeholder group are the stakeholders within the small-scale cyber security ecosystem who are voicing concern over the level of cyber security achieved by SMEs. There are three main arguments given for concern over SME cyber security:

1. The suggestion that SMEs are being used as attack vectors for large companies or government departments higher up the supply chain [119].

2. Attacks reported by SMEs in surveys such as the UK Department for Business Innovation and Skills (BIS) Information Security Breaches Survey [110].

3. The political moral incentive — the risk of financial loss from cyber incidents versus the number of SMEs in the UK, the percentage of the GDP they account for and the amount of employment they provide[2].

The concerns stated above have been the drivers for various SME security initiatives. Past initiatives include ENISA's Risk Assessment and Risk Management Methods: Information Packages for SMEs (March 2006) [33]. The ENISA information package is still available and describes a risk analysis process in accessible language. The issue is

2 www.computerweekly.com/news/2240184456/Small-firms-lose-up-to-800m-to-cyber-crime-says-FSB

with the way the advice is framed as business processes, audits and with only high-infrastructure organisations (with offices, physical network infrastructure and servers, etc.) given in the case studies — a scenario SMEs increasingly struggle to identify with.

UK Government initiatives launched in reaction to the 2011 National Cyber Security Strategy [109] include the Cyber Security Voucher Scheme[3], Cyber Aware[4] and Cyber Essentials [111], and are slightly more varied in their approaches and development process. In line with the research on cyber security advice completed by Renaud [86], the number of sources of information have gradually been honed and reduced to ensure that SSITUs are provided with a consistent message. Despite this, SSITU cyber security remains a significant challenge in the 2016 UK National Cyber Security Strategy [115].

The mixed success of past initiatives may signify a need for more extensive SME participation in the planning and development of advice. However, there are also industry-led initiatives, from professional membership groups adapting government advice to fit their sector [67], to SMEs such as IASME[5] developing standards specifically adapted to smaller organisations.

While a level of support for SMEs wanting to implement cyber security exists, the *incentives* supplied to SMEs are not as well evolved. What is largely driving concern are risks and requirements owned by *large* organisations, prompting this definition of a *risk-holding* stakeholder group.

Some risk holders, for example the UK Government, are also becoming *security providers*, supplying advice, the capacity to share threat intelligence and frameworks for accrediting experts in the hope of securing their own supply chains.

2.1.5 *Security providers*

There are three types of *security provider* considered in this dissertation:

1. Knowledge providers — government or membership organisations with initiatives intended to increase awareness or recommend specific security measures.

2. Stand-alone security providers — organisations selling security products.

3. Product-embedded security providers — organisations selling secure products or services (or products/services containing some security measures).

In Chapters 4 and 5 we describe how security providers play a key role in the small-scale cyber security ecosystem. Stand-alone security providers considered in this dissertation are those whose brands are typically recognised by a home user — Sophos[6], McAfee[7], Norton[8], etc. Product-embedded security providers may also be recognisable brands to the SSITU group — the security of third-party software has become so key to the reputation of platform providers that Microsoft offers free advice to developers

3 Innovation vouchers for SMEs, which were available from October 2015 and managed by innovateuk.org
4 www.cyberaware.gov.uk
5 www.iasme.co.uk
6 www.sophos.com
7 www.mcafee.com/uk/index.html
8 uk.norton.com

about the security development lifecycle[9] and Google are threatening to create a public list of hardware partners who are slow in updating the Android operating system[10].

The most complex role within the small-scale cyber security ecosystem is that of knowledge providers. Training is another product offered by security providers, but, as discussed in Section 2.1.4, there is a variety of training and advice provided to SSITUs for free.

2.2 The representation of SSITUs in the academic literature

2.2.1 *SMEs*

SMEs, home users and charities are not entirely unrepresented in the cyber security literature, although the present author has not found examples of SSITUs being examined as a single cyber security user group. SMEs are, though, under-represented in the literature. This is felt to be a consequence of a reluctance from SMEs to interact with researchers, standards development and workshops. Identifying participants is known to be challenging for any type of empirical cyber security research [18]. SME engagement is also not a problem unique to cyber security research [56, 127], a state of affairs replicated by an initial SME-focused project [76] and in initiatives later described by our participants. It is this issue that drove the methodology we describe in Chapter 3.

Some other studies about security in SMEs focus on a smaller number of organisations, using responses from multiple roles in the same organisation. For example, [54] evaluates the use of security metrics within SMEs using a sample group comprised of 85.6% medium-sized companies, so that they can compare the types of metrics needed by managers against those needed by the IT function. This approach under-represents the smallest SMEs, who make up 95% of businesses in the UK [28], and who are less likely to have a separation between IT and decision-making roles.

In the UK a large proportion of information and advice for SMEs is provided by the Government [111, 112] or builds on and contextualises government advice for a specific sector [67] (a more in-depth discussion about the advice developed by the UK Government can be found in Chapter 5).

Research into SME cyber security has been carried out in parallel to this study by other projects. For example, the roadmap for RISCS[11] includes developing empirical cyber security research that would be relevant to SMEs, and research is being carried out at Strathclyde University [86], Imperial College London [34] and University College London [78].

Renaud describes SME cyber security awareness in Scotland, discussing the sheer number of sources of often conflicting advice described by participants and concluding that, in order for awareness initiatives to be successful, they need to have a clear and unified message irrespective of the source [86]. Her questionnaire-based research design has similarities to our initial study and is discussed in Chapter 3. She also describes a model of threat management that both aligns business decision making with

9 www.microsoft.com/en-us/sdl/

10 www.bloomberg.com/news/articles/2016-05-25/google-steps-up-pressure-on-partners-tardy-in-updating-android

11 www.riscs.org.uk

Rhee et al.'s description of end user self-efficacy [87], but also enriches findings from our initial study [76].

The model of threat management described by Renaud illustrates an SME's need to begin addressing cyber security threats by anticipating that they have a *realistic* appraisal of the threat and a realistic chance of response efficacy [86]. She provides multiple paths where SMEs react by controlling their fear by downplaying an insurmountable risk.

In [34] Fielder et al. provide a decision support tool that provides advice on optimising cyber security budgets for SMEs when implementing the basic security measures suggested by the UK Government and is relevant to our discussion about risk and decision making in Chapter 4. They conclude that their approach can only model fairly simple security issues, as more complex scenarios would result in results that are too complex to evaluate, but highlight the importance of understanding the indirect costs of SMEs implementing security.

Parkin et al. use archetypes developed from "the experiences of a partner company", which are similar to those we describe in Chapter 5, in a model intended to measure and limit the security burden placed on staff [78]. One reason for the similarities is their reference to architecture descriptions published in our initial study [76], but they also highlight key characteristics of SMEs, for example, limited resources and cyber security decision making by staff with limited knowledge, which validates some of the SME attributes highlighted in Chapters 4–6.

They suggest that the security burden placed on staff ultimately leads to indirect costs and so enumerate human-factors as an "available responsibility budget" [78]. Their model focuses on reducing an organisation's exposure to data breaches and uses information drawn from an SME collaborator to make suggestions within a realistic context. Their main suggestion is that 2-factor authentication would be achievable for the majority of SMEs. Although the results of this study are interesting and relevant to our study, the case study of n=1 means that further exploration of the problem is warranted.

One recent UK Government and KPMG survey also evaluated the link between SMEs' reputations and cyber security [49]. They show how less than a quarter of SMEs treat cyber security as a top concern, massively underestimating the cost of a breach, the disruption in quality of service and its long term impact. In contrast they provide figures from the supply chain, highlighting the likelihood that 58% of consumers would be discouraged from using a company if they suffered a breach, 86% of procurement managers would remove those companies from their roster and 94% of procurement managers see cyber security standards as a differentiator. Although details of the methodology used to produce this publication are scarce and the questions asked may include a bias from the RH stakeholder group, this difference in perspectives reinforces Renaud's conclusions about the potential complacency of SMEs.

2.2.2 *Individuals*

Individual users are better represented in the literature than other SSITUs. There are papers on decision making, usability and self efficacy [35, 50, 87], and using technology for personal or work reasons [132]. There is, however, a lack of focus on one of the most important phenomena we have drawn out of the data — the extent to which small

business owners struggle with multi-purpose networks and the conflicts of interest these produce when defining policies.

Kritzinger and von Solms discuss the vulnerability of home users to cyber attacks, proposing to address this problem by 'forcing' users to learn about cyber risk [50]. Their theoretical model suggests that the Internet Service Provider (ISP) should act as a regulating service, empowering the user with cyber security knowledge. The ISP provides a portal, providing up-to-date threat awareness training with integrated user assessments. They suggest that to ensure that users become knowledgeable about security there needs to be an element of enforcement — users are both tested on their knowledge and their internet access is limited until they have sufficient insight to avoid risks.

Flechais et al. highlight the lack of compatibility between *secure* systems and *usable* systems [35]. Their focus is on integrating cyber security processes into the development of usable technology and they provide some useful insight into the burden placed on developers to provide usable secure systems. Their approach makes security more systematic, and so easier for developers to approach. They also advocate involving stakeholders in security planning processes as an effective means to increase knowledge and commitment — an observation relevant to our discussion around SMEs' lack of engagement and government becoming a security provider in Chapter 4.

Rhee et al. explore when users display self-efficacy and the effect of a successful attack on that efficacy [87]. They describe how users can develop confidence in their ability to implement cyber security measures, however, after an incident this self-efficacy is damaged and can lead to a reduced engagement with security. In addition to Renaud's discussion around threat management, where SME owners choose to downplay unassailable risks, in this case users are demoralised post-breach by their failure to secure — if they remain vulnerable why invest in security? Rhee concludes that low-key support from IT providers can reduce the impact of a breach on self-efficacy, encouraging users to maintain their security practices. One criticism of this research, in the context of our study, is that the participants evaluated were part of a large organisation (graduate students) — while it reflects an end user behaviour it does not offer solutions that are easily accessible to SSITUs.

Cormac Herley provides the counterpoint, discussing why users fail to implement simple cyber security measures [42] and, more recently, discussing the barriers to progress [43]. He suggests that even the 'basic' security measures users are advised to implement produce such a significant cognitive burden that the cost-benefit analysis opposes their implementation [42]. Indirect costs and an understanding of user context becomes a recurrent theme in the discussion of cyber security across the entire SSITU stakeholder group. Herley suggests that the lack of progress improving users' engagement with security is due to the lack of adaptability of security measures to a 'low-assurance' marketplace (SSITUs) and a failure to address the cost-benefit analysis where users still benefit from *not* engaging with security [43]. He concludes that being more persistent in providing complex advice will not produce the desired effect, meaning that advice (and the associated measures) need to become more usable.

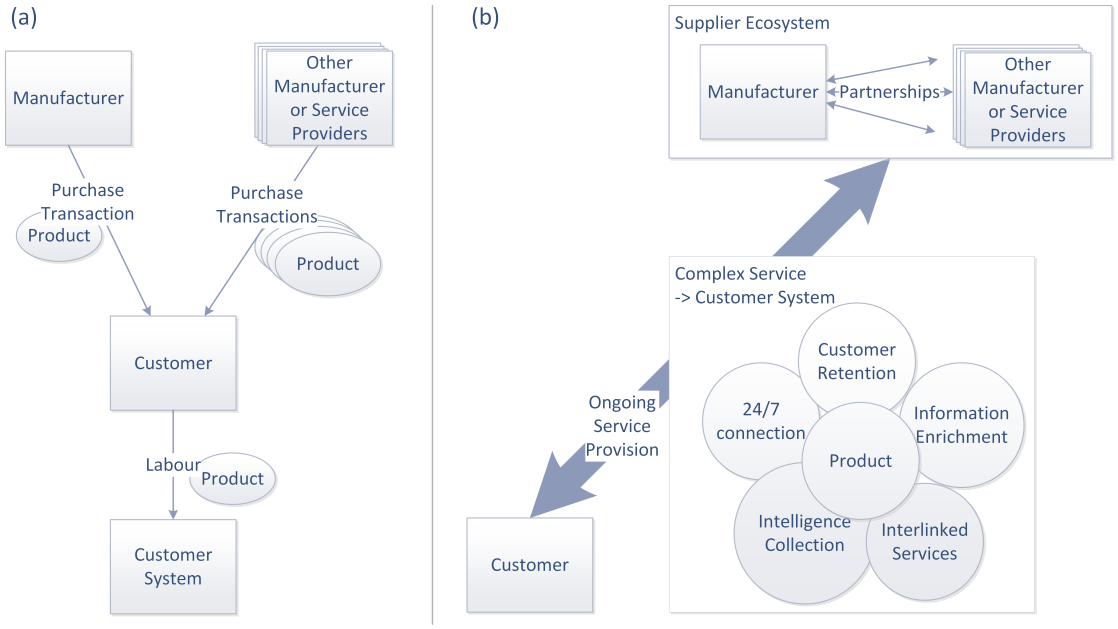


Figure 4: *(a) A traditional product business model; and (b) an IT-driven business model*

2.2.3 *Other SSITUs*

We have found no academic contributions considering the needs of startups differently to those of slower-growth SMEs, although security providers are beginning to cater specifically to this sector[12]. Small charities are also under-represented in the literature, although one paper highlighting the disproportionately high cyber threats faced by small NGOs carrying out politically sensitive work [92] is used as a differentiator in our exploration of cyber threats in Chapter 4.

2.3 BUSINESS MODELS FOR CONSUMER TECHNOLOGY

As described in the Section 2.2, SSITUs make decisions as small stakeholders with limited technology knowledge. The consumer marketplace's evolution towards IT-driven business models becomes a key influencer of SSITU technology use. This section describes some key elements in the evolution of these business models and the supply chain complexity it creates.

Figure 4 provides an illustrated breakdown of the differences between the typical product manufacture business model and the more service-focussed IT-driven business model. Traditionally, as depicted in Figure 4 (a), a consumer buys a variety of products and services. The consumer may choose to do some work once they've purchased a product to integrate it into a system, or their system may consist of a variety of items whose only connection is the consumer using them. Kagermann et al. [46] suggest that over time this business model is becoming increasingly less profitable, leading to IT-driven business models: almost every interaction we now have in shops, restaurants, at work and through advertising includes a link to a company's on-line presence; at every opportunity, businesses are attempting to open a continued dialogue with their

12 certificationeurope.co.uk/start-secure/

customers whether through the official web-site or via a social media presence. To a great extent, these models are shaped by customer value.

In the context of IT-driven business models, manufacturers make money by reducing the cognitive workload of the consumer as the customer system can be pre-built and configured (Figure 4 (b)). This is of great importance where SSITUs are reliant on technology without having much knowledge of its functionality or configuration. Without IT-driven business models usability would be reduced to the point that IT use would be limited by the computer-literacy of the end user.

The most mature implementations of this business model are in the IT sector itself where PC or mobile device manufacturers form partnerships with operating system and software development companies. These partnerships allow products to be sold ready to use 'out-of-the-box' and let consumers try various software before they buy.

In altering their business model to that of a service provider, manufacturers hope to increase reliability, as design standards are agreed within the supplier ecosystem. They also aim to improve customer retention by deliberately building in reasons for continued interaction with the consumer. All of these services depend on the product going on-line — which might be characterised as *interconnectivity by design*.

This updating of existing consumer products with apps and gadgets is in contrast to an Industrial Control System (ICS) or a smart grid scenario, where pre-existing systems are put on-line in order to reduce monitoring costs, for example [130], and contributes to the relevance of SSITU cyber security to consumer privacy concerns (as discussed in Section 2.6).

The issue with this business model is that it is drawing manufacturers away from their area of expertise and into a highly complex ecosystem where it becomes difficult to define responsibility adequately to produce the accountability required by, for example, the new General Data Protection Regulation (GDPR) [103]. It can also produce what van Eeten and Bauer term *network externalities*, where interdependence impacts on other stakeholders, either by removing a vulnerability, or by one stakeholder reducing their vulnerability to the extent that they increase the threat to other stakeholders [119].

New elements of the product or service may be seen as a fairly modular element of the design, with the possibility of outsourcing the development of applications, web portals, etc. to third parties. While modular design may help manufacturers when developing a complex system, this modularity of both the product and development teams makes it far more difficult for any stakeholder in the supply chain to judge the risks associated with the use of the system once it is connected.

2.4 INCUMBENT CYBER SECURITY PRACTICES

Computer security has converged with other technology or information-related processes to result in cyber security core principles. However, in our move from computer security, information assurance, etc. towards cyber security, Von Solms and van Niekerk [121] suggest that we have fundamentally changed the scope of responsibility. Cyber security moves from protecting computer-related or information assets towards protecting the business processes and the user confidence that underpins a digital economy.

Certain principles, such as the goal of achieving adequate levels of confidentiality, integrity and availability for a specific company, system or asset, are universal. For example, the ISO 27000 standard [3] defines the CIA triad as:

- *Confidentiality:* "property that information is not made available or disclosed to unauthorized individuals, entities, or processes"
- *Integrity:* "property of accuracy and completeness"
- *Availability:* "property of being accessible and usable upon demand by an authorized entity"

The language used in the implementation of these main goals of cyber security differs depending on the audience they are communicating with, but there are recurrent themes, which taken together can begin to describe the current perception of cyber security 'best practices'.

Figure 5 provides an amalgamated overview of the cyber principles developed from examples by organisations with different perspectives[13], namely:

1. NIST (standardised security functions [65])
2. $(ISC)^2$ (professional competencies [38])
3. SABSA (enterprise security architecture[14])
4. GDPR (privacy legislation [103])
5. Cyber Essentials (a cyber security standard aimed at SMEs [111])

The intention is to highlight and categorise key principles within the cyber security lifecycle made from a variety of perspectives. In the case of 1–3 the core principles from each approach have been included in the overview and, although it would be infeasible to include every subcategory in this figure, the lifecycle is enhanced by the addition of certain subcategories of principle (highlighted in the illustration by dashed boxes).

The General Data Protection Regulation (GDPR) also describes principles [103]. Of the eight principles, the majority relate to business processes outside of the scope of this discussion (privacy is discussed in Section 2.6). However, there are three which do influence the perception of cyber security good practice — the overarching principle of "lawfulness, fairness and transparency" (GDPR as an example of legal rules influencing business context), as well as principles of "integrity and confidentiality" (influencing the application of 'appropriate' measures) and "accountability" (influencing the documentation of cyber security processes to demonstrate compliance). Subcategories of principles are described in the GDPR as Articles relating to various stakeholders, some of which are relevant to cyber security best practices (also included as dashed boxes).

Finally, Cyber Essentials has been included to provide an overview of cyber security best practices *for SSITUs* as described by the UK Government. In line with Renaud's

13 The International Standards Organisation's contribution (the ISO 27000 series, which is likely to have amalgamated perspectives from diverse sectors, as well as being aligned with the more general ISO 31000 standards on Risk Management [9], and so be less useful in this comparative discussion) is cited later in this section.

14 www.sabsa.org/white_paper

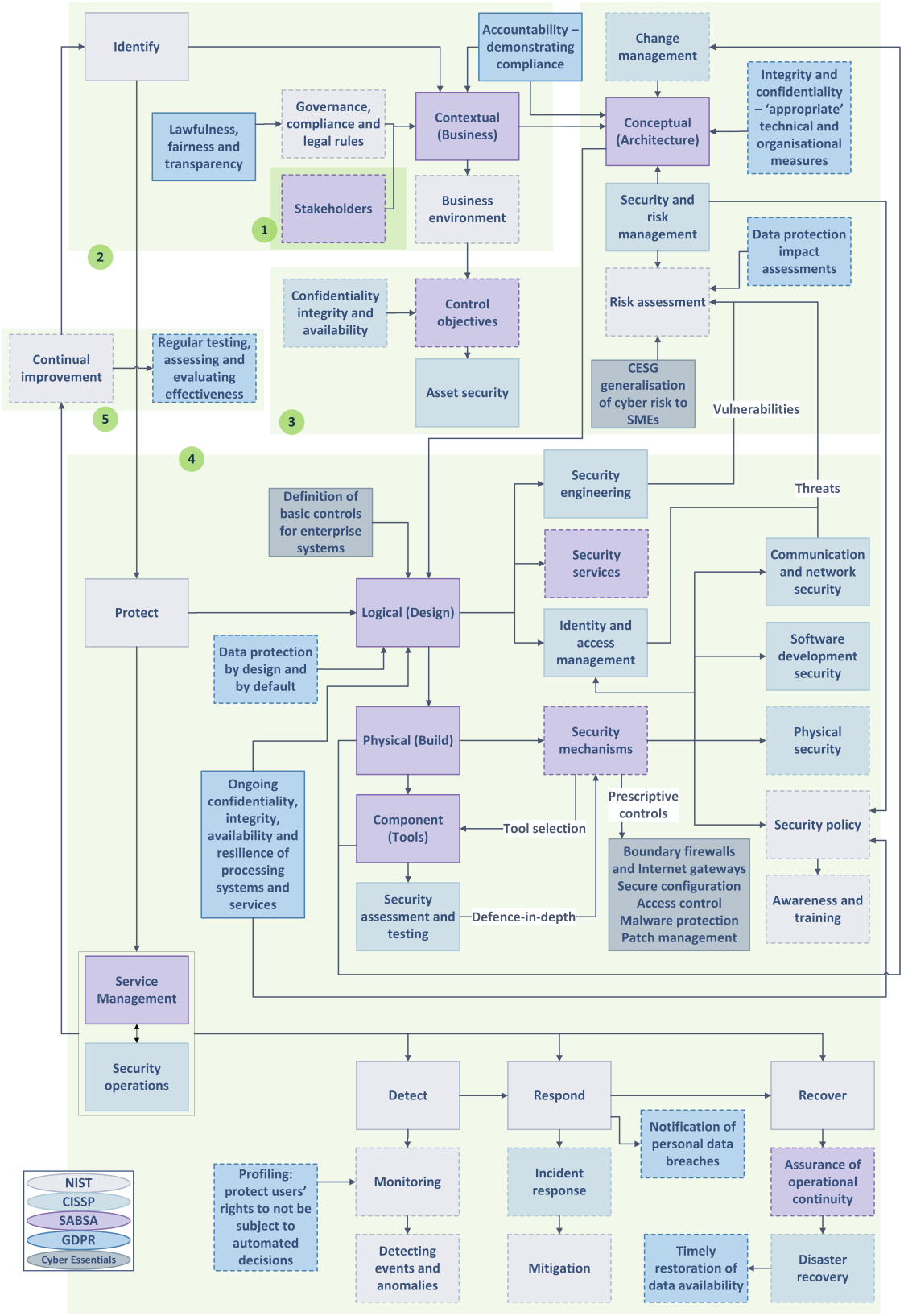


Figure 5: *A categorisation of cyber principles developed from the perspectives of technology standards (NIST); enterprise architecture practices (SABSA); professional training (CISSP); legislation (GDPR); and a standard aimed at SMEs (Cyber Essentials)*

recommendation [86] this is now a consistent message being offered to SSITUs from a diverse number of sources.

Reviewed together, and with the exception of Cyber Essentials, these properties align with security architecture models such as defence-in-depth [25] and defence-in-breadth [15], which aim to make security more comprehensive and resilient to threats, either within a single organisation or across a supply chain. The principles can be grouped into five categories (highlighted by numbered green boxes in Figure 5), which also align with core concepts of ISO 27001 [4], namely: organisational context (category 2); leadership (1); planning (3); support (4); operation (4); performance evaluation (4); and improvement (5). The main insight this analysis provides is in the distribution of principles from each source (each represented by a different colour) across the five categories.

Cyber Essentials, the only example developed with accessibility to SSITUs in mind, sidesteps some areas of cyber security principles in favour of a prescriptive set of measures that can be linked back to risks identified by the UK Government [111]. As such, from the SSITU's perspective it only has a presence in category 4 (principles relating to the application of cyber security measures). Figure 5 does include a reference to Cyber Essentials in the planning section, to recognise the research carried out by the UK Government to quantify risk on SSITUs' behalves prior to developing the standard. The question is, with their aim of producing *achievable* guidelines, have the UK Government produced something that is insufficient for both SSITUs and RH stakeholders to achieve 'appropriate' levels of security as perceived by other contributors to cyber security best practices?

What is also evident from the description of cyber security principles in the examples explored in this section, is that more mainstream security advice is neither technology nor business process agnostic. For example, the breadth of skills required to carry out all security roles necessitates a minimum number of employees and elements such as network security or cyber security risk assessment imply a level of system ownership not always possible for SSITUs.

Cyber security experts begin with an expectation of what an IT system looks like when they develop cyber security principles, which, owing to their greater experience working with large organisations, is best adapted to larger organisations.

However, when we bring this description of large-scale corporate cyber security best practices together with the contributions of Chapters 4 and 5 for comparison in Chapter 6, the gap between a risk holder's expectations and the realities of the SSITUs' operational environments becomes evident.

2.5 SAFETY ENGINEERING

Safety differs from security in that, while both aim to prevent something 'bad' from happening, safety engineering tends to focus on the potential for and prevention of *accidental* harm, while security typically focuses on malicious threats. This section describes key factors of safety engineering best practices, which, with the predicted growth of the Internet of Things, assists in our discussion of emerging threats in Chapter 5.

The *SEMA* referential framework of [83] has such distinctions at its heart:

- *System vs. Environment (S-E) distinction*: "Security is concerned with the risks originating from the environment and potentially impacting the system, whereas safety deals with the risks arising from the system and potentially impacting the environment." [83]
- *Malicious vs. Accidental (M-A) distinction*: "Security typically addresses malicious risks while safety addresses purely accidental risks." [83]

The EU directive on general product safety defines a "safe product" as follows [102]:

> "'*safe product*' shall mean any product which, under normal or reasonably foreseeable conditions of use including duration and, where applicable, putting into service, installation and maintenance requirements, does not present any risk or only the minimum risks compatible with the product's use, considered to be acceptable and consistent with a high level of protection for the safety and health of persons, taking into account the following points in particular:
>
> i. the characteristics of the product, including its composition, packaging, instructions for assembly and, where applicable, for installation and maintenance;
>
> ii. the effect on other products, where it is reasonably foreseeable that it will be used with other products;
>
> iii. the presentation of the product, the labelling, any warnings and instructions for its use and disposal and any other indication or information regarding the product;
>
> iv. the categories of consumers at risk when using the product, in particular children and the elderly.
>
> The feasibility of obtaining higher levels of safety or the availability of other products presenting a lesser degree of risk shall not constitute grounds for considering a product to be 'dangerous'."

Under EU and UK law, manufacturers have an obligation to guarantee safety [100], as well as to adhere to consumer rights legislation [113]. Safety is a heavily regulated subject in engineering standards and product liability at both a national and European level, e.g. [7, 2, 8, 10]. Legislation typically refers to a set of standards dictating the interpretation of a law in a specific context (the sector or product constituents).

Where standards fail to be prescriptive about how a design issue should be dealt with, the fallback position is that products should be designed following good engineering practice [100]. Good engineering practice in such a cross-disciplinary field is probably fairly open to interpretation; however, texts such as those by Storey [97] and Leveson [53], which describe the traditional approach to safety, in what has now become the field of cyber physical systems, provide excellent starting points. Figure 6 provides an overview of how different consumer protection legislation and safety practices interact. It illustrates how the far more mature consumer safety practices fail to

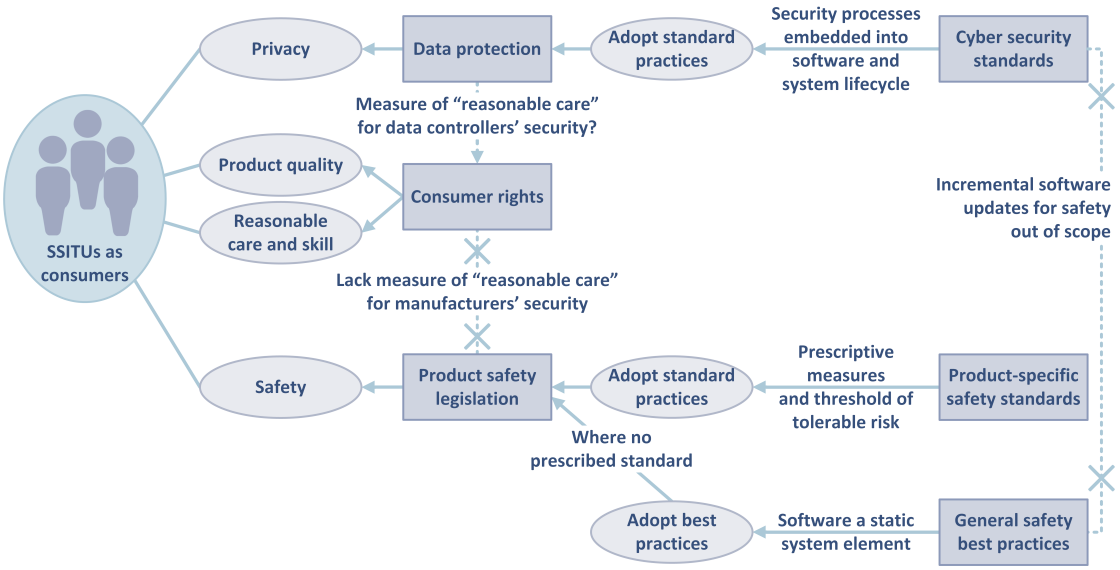


Figure 6: *An overview of the interaction between safety in legislation and best practices*

be replicated or assimilated by newer technology-related practices. The potential pitfalls of this lack of integration of engineering processes and consumer expectations is discussed in Chapter 5.

In the traditional approach to safety, products are ideally designed to be intrinsically safe — meaning that they can't produce enough energy to cause harm. An example of this is the safety requirements for IT equipment [10]. Where this isn't possible, a threshold of tolerable risk has to be defined, and measures put in place throughout the design and verification processes to ensure that potential hazards are not likely enough to reach this threshold [97]. In safety engineering software faults are considered design issues, as algorithms do not degrade over time in the way that electrical components do. This means that software has to be rigorously validated and verified as part of the design process, but as code does not change software is not usually re-evaluated over time.

A recent contribution by Pièrre-Cambacédès and Bouissou [82] provides an authoritative survey of the transfusion of techniques as safety and security processes converge. The motivation for the 'merging' of the two fields is discussed in [79]:

> "In future, more and more IT-systems will be both, safety- and security-critical. The reason for this is that IT-systems are embedded in ever more influential parts of our living- and working environment and that these embedded IT-systems are networked — be it to enhance their functionality now (or just as an option for future use), be it to ease maintenance." [79]

Cyber security issues are not a new phenomenon in hazardous environments. Established standards have been updated to reflect new threats; for example, the MoD standard for safety management in defence systems now includes a section on cyber security and data integrity [1]. Contractors supplying products, services and/or systems have to consider cyber security in the context of safety where breaches, or (due to increased dependence on data) data integrity issues, may be a contributory cause of hazards or failure modes. Consumer standards are yet to (and may never wish to) repli-

cate this level of security requirement, but the evolution of these standards provide an interesting precedent.

Regulations such as product liability law [100], consumer rights [113] and safety standards have been embedded in every product bought in the UK, having in many cases been developed over decades. While customers only expect IT systems to provide a best-effort service, they (reasonably) expect everything they buy to be intrinsically safe to use. This difference in expectations, in combination with data protection requirements, may become a catalyst for manufacturers to change the way they approach cyber security in consumer products.

2.6 PRIVACY

Privacy intersects with all of the other themes influencing SSITUs' cyber security practices. Privacy regulations, and practices that could protect a users' privacy, play an important role in understanding the potential conflicts of interest SSITUs have as cyber security decision makers. The background information provided in this section provides context to our discussions in Chapter 5 around the digital footprint.

The data economy incentivises the collection and sale of personal data, and privacy legislation has become de facto best practice for anyone processing personal information — unless a company is using privacy as a key selling point for its services (for example, TOR[15]).

Privacy legislation in Europe has been influenced by principles developed in 1980 by the OECD (the Organization for Economic Cooperation and Development):[16]

1. *"Collection Limitation Principle"*: collection should be limited, obtained by lawful means and usually with consent.
2. *"Data Quality Principle"*: data held should be relevant to their use accurate and up-to-date.
3. *"Purpose Specification Principle"*: data should only collected for purposes disclosed to the subject pre-consent.
4. *"Use Limitation Principle"*: data should only used or shared for purposes the subject has consented to, or by the authority of law.
5. *"Security Safeguards Principle"*: personal data should be protected by reasonable security measures.
6. *"Openness Principle"*: data subjects should have access to information about how their data is being used and details of the data controller.
7. *"Individual Participation Principle"*: data subjects should be able to request information related to data held about them and to request its deletion or amendment if this data is inaccurate.
8. *"Accountability Principle"*: data controllers are accountable for applying the measures to ensure privacy.

15 www.torproject.org/
16 oecdprivacy.org/

These principles were incorporated into the EU Data Protection Directive [101], which was part of both privacy and human rights law and directed governments to implement data protection law in each country. The directive was adopted in the UK via the Data Protection Act [107]. The data protection act *"controls how personal information is used by organisations, businesses or the government"* and the principles summarised in [114] show a resemblance to the OECD principles described above.

The Data Protection Act defines personal data as:

> "'personal data' means data which relate to a living individual who can be identified — (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual." [107]

The new EU data protection regulation (GDPR) (*"on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) "* [103], came into force on the 24th of May 2016 and applied from the 25th of May 2018[17]. This regulation applies automatically to all member states and the harmonisation of data processing across the EU is seen as an advantage in developing a digital single market[18].

This new regulation is intended to give users more control over their personal data in order to *"strengthen citizens' rights and build trust"*, in reaction to concerns held by EU citizens about data collection without consent and the use of those data [103]. There are five main ways that the new regulations intend to improve users control over privacy:

1. Formalising the "right to be forgotten" so that users can request data be deleted once it is obsolete.
2. Users should be able to get accessible information about how their data is processed and now have the *right to data portability* to facilitate the transfer of information between service providers.
3. Users have the right to know when their data has been hacked and organisations have to inform a national supervisory authority.
4. Data protection will be built into all services by design with privacy-protecting options set as default.
5. Enforcement is stronger with a new principle of 'accountability' and fines for non-compliance up to 4% of an organisation's global annual turnover [103].

Privacy legislation's approach to cyber security plays into the dialogue around SSITU security in a few ways — first, because, as illustrated in Figure 6, the secure practices described by privacy legislation are aligned with cyber security industry best practices. The GDPR is not technology-agnostic: it makes assumptions about the quality of cyber security a data controller can achieve based only on the level of protection they require

17 ec.europa.eu/justice/data-protection/reform/index_en.htm

18 Despite the 23 June 2016 referendum on membership of the EU, UK businesses are still required to comply with the EU's General Data Protection Regulation. This means that the GDPR, and its associated cyber security requirements, remain relevant to the research carried out in this dissertation.

the consumer to have. For example, the now mandatory Privacy Impact Assessments (which are required to satisfy the principle of accountability) are compatible with cyber security risk assessment processes; however, as we will discuss in Chapter 4, the compatibility of cyber security risk assessments with SSITUs' business processes is questionable.

Secondly, to a large extent all applications of privacy engineering best practice include the concept of consent, leaving the decision to reduce privacy with the users. SSITUs are likely to have conflicts of interest in the way they need to balance privacy as an individual and security in their professional roles, often within the same device. This is discussed in more detail in Chapter 5.

Finally, as with the interaction between cyber security and safety described in Sections 2.4 and 2.5, there is an interaction between the physical aspects of security and privacy decisions — the impact of the availability of data on physical threats such as stalking, grooming or bullying. In this case SSITUs' ability to make privacy-conscious decisions could impact their well-being.

2.7 SUMMARY

In this chapter we have defined the small-scale cyber security stakeholder groups, including subsets of the SSITU group. This was followed by a broad literature survey, encompassing both the representation of SSITUs in the academic literature and the incumbent practices that may be found to influence their interaction with cyber security. The literature survey will facilitate a comparative analysis with the data provided by our participants in later chapters. In the next chapter we will outline the methodology used to develop the contributions of this dissertation.

3

METHODOLOGY

In this chapter we introduce the methodology used to underpin the research described in this dissertation, informed by approaches such as Grounded Theory and Requirements Engineering. We highlight how they are combined and used to drive and validate the contributions of this dissertation.

The remainder of the chapter outlines the project design as follows. Section 3.1 describes how our participants have shaped our research design. Section 3.2 describes the data collected in this study. The generation of a UK case study from the dataset is described in Section 3.3. In Section 3.4 we discuss how a requirements engineering process and the UK case study were used to structure a small-scale cyber security requirements framework. Section 3.5 discusses the validity of the project design, before Section 3.6 concludes the chapter.

3.1 SSITUS AND THEIR INFLUENCE ON PROJECT DESIGN

The aim of this research was to use empirical methods 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.

The difficulties in gaining access to the Small to Medium Enterprise (SME) user group highlighted in Chapter 2 have influenced our project design. Small organisations typically don't have the resources available to expend time engaging with research and incentives typically offered to individuals to participate — paying participants or giving them a chance to win something — provided no *business* reason to participate.

Attempts at random sampling in an initial study intended to gather information about cyber security practices in SMEs resulted in a response rate of less than 1% [76]. The majority of responses originated from advertising the study on social media or making direct requests to business acquaintances. For this reason our 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 way small businesses use technology.

As such, we take a *qualitative* approach, similar to that employed by [12] and [61], employing a meta-study of the sector, which combines the results of our empirical study with recent results from different fields of research and the views of several different stakeholder groups.

Recruiting a smaller group of participants to provide in-depth qualitative data about cyber security in the small-scale IT user group was achievable, where the collection of a large quantitative dataset would not have been feasible. Questionnaires and interviews, rather than more time-intensive collection methods such as observation, were used to reduce the commitment requested of any one participant in these resource-constrained organisations.

The incentive to participate had to be in the form of small-scale partnerships. In exchange for their time we retained contact with the participants providing tailored

updates about the research outcomes, aligning our methodology with the business needs of the participants, without introducing a large administrative burden on any one participant. A more in-depth reflection on how we managed to engage SMEs in research can be found in Chapter 7.

3.2 DATA

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. There were 33 respondents in the initial questionnaire dataset (the questions can be found in Appendix A), 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[1].

The outcomes of the study carried out using this initial dataset [76] suggested that a valuable contribution could be made to the sector by a more in-depth study, using that first collection of results (from a specific population — SMEs) to guide the definition of the user group for whom the existing cyber security practices are ill-adapted (the small-scale cyber security stakeholders defined in Chapter 2).

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 encompassing 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 our SSITU stakeholder groups.

Due to our qualitative approach sampling was *theoretical*, rather than random [23]. Eisendhart suggests that the use of theoretical sampling *"Focuses efforts on theoretically useful cases — i.e., those that replicate or extend theory by filling conceptual categories"* [31]. We followed the recommendation of Guest et al. [39] to conduct 12–20 interviews, and participants were recruited to assist in our identification of the themes that help describe the small-scale cyber security ecosystem — with the aim being to develop a breadth of understanding.

The non-prescriptive structure of the interviews was to obtain an enhanced level of detail from participants and allow participants from different backgrounds within the stakeholder group to contribute. Every participant was asked about their role and experiences in cyber security in order to put all of the interviews into context.

In some interviews (8 of 20) participants talked about multiple organisations/cyber security contexts — 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 8 provides an overview of the interview participants — the stakeholder group(s) they represent, their background and information on the technical skills (TS — low (L) or high (H) — based on whether the participant

1 The results of this initial feasibility study can be found in [76] with a detailed description of the methodology in an extended technical report: http://ora.ox.ac.uk/objects/uuid:4363144b-5667-4fdd-8cd3-b8e35436107e

reported having a technical background) each participant had when making decisions about cyber security.

The interviews took place over an eight-month period, beginning in October 2014. The projects were ethically approved by Oxford University Central University Research Ethics Committee. Interviews were carried out confidentially and field notes were used to record questions and responses. Additional reflections and observations about the interviews were documented immediately after the interviews, as very few participants agreed to be audio-recorded.

Where relevant, we also make use of secondary data sources, such as the descriptions of SME data breaches provided in the Monetary Penalty Notices issued by the UK Information Commissioner's Office[2].

3.3 GENERATING THE UK CASE STUDY

3.3.1 *Data analysis*

The insights we share throughout Chapters 4 and 5 are the result of a Grounded Theory analysis of our dataset. Grounded Theory is an inductive theory generating process rather than a theory-testing methodology, by which we mean that we were not required to develop a hypothesis in the preparatory phase of the project — an advantage when researching a subject where there are limited existing data from the perspective of a particular stakeholder group.

Grounded Theory does not begin with a theory in mind — instead 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. Corbin and Strauss describe it as a methodology that facilitates *"building theory from data"* although they go on to add that they typically use the term in a more generic way to *"denote theoretical constructs derived from qualitative analysis of data"* [26].

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. The process (illustrated in Figure 8) involves the breaking down of data using an open coding process to identify concepts. Those concepts are then reassembled during the axial coding process to define categories or phenomena. Finally in the selective coding process a core category is identified, which pulls all the other phenomena together into an "explanatory whole". Where required, additional data was collected to introduce new themes that assist in the development of a theory.

Table 3 provides a summary of the codes, concepts and phenomena that emerged from the analysis, with a full coding table available in Appendix C. In total 9 phenomena emerged, including the SSITU profile itself, encompassing 29 concepts and 87 individual codes. These phenomena were used in the development of Chapters 4 & 5, providing us with the structure needed to discuss the emerging theory. This emerging theory of *how SSITUs approach cyber security* was split into two narratives: justifying cyber security investment; and implementing cyber security, to improve readability in the dissertation. A table, showing the subset of phenomena and concepts discussed, is presented at the beginning of these chapters so that research outcomes can be mapped back to the coding table.

2 ico.org.uk/action-weve-taken

Data Source	SSITU	SP	RH	TS	Description
Questionnaire	33			≈60% L	SMEs
Interview 1	•			H	Home-working medium-sized company director
Interview 2		•	•	H	Security design at large manufacturer
Interview 3	•			H	Father of a family with young children
Interview 4	•			L	Single person company operating from the family home
Interview 5	•	•		L	Company director with multiple micro-companies
Interview 6	•	•		L	Cyber Essentials accreditor
Interview 7		•		L	Large organisation facilitating an innovation centre
Interview 8	•	•		H	Small IT service provider
Interview 9		•	•	L	UK civil servant tasked with increasing cyber awareness
Interview 10		•		H	Professional membership organisation providing IT advice
Interview 11			•	H	CISO in a large critical infrastructure organisation
Interview 12		•		L	UK law enforcement (national) — policy
Interview 13		•	•	L	UK Government cyber incidents and information sharing
Interview 14	•			H	Infrastructure manager of a small software development and data hosting company
Interview 15		•		H	UK law enforcement (national) — investigator
Interview 16	•			H	Privacy conscious individual with work BYOD policy
Interview 17	•			L	Individual (student) in a multiple-household home
Interview 18			•	H	Consumer safety expert on the introduction of cyber risk
Interview 19	•	•		H	Web developer volunteering for multiple clubs and charities
Interview 20		•		L	UK law enforcement (regional police force) — community policing

Table 2: *Dataset overview*

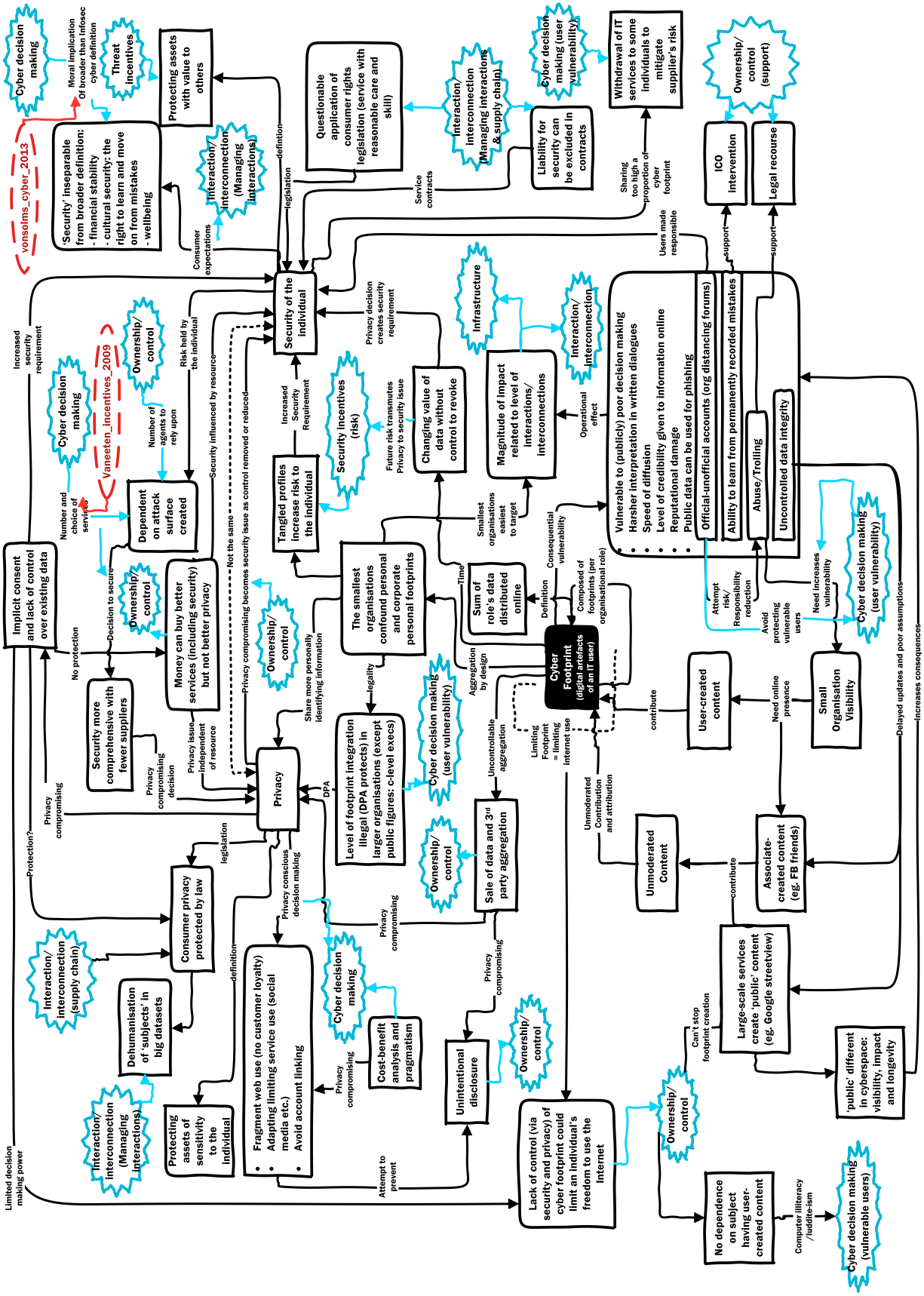


Figure 7: *A sample of the diagrams produced during axial coding*

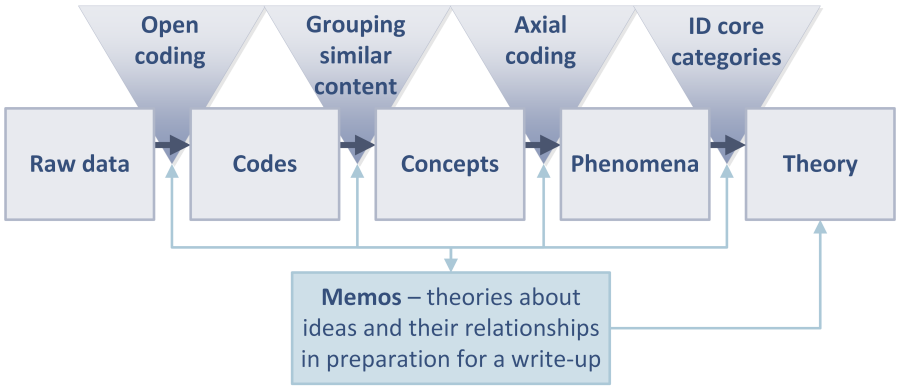


Figure 8: *An overview of the Grounded Theory analysis process*

A sample diagram, created to explore emerging phenomena during the axial coding process can be seen in Figure 7. It shows how the ideas categorised by codes and concepts were drawn together to develop a narrative (in this case the 'digital footprint' section of Chapter 5).

The application of Grounded Theory in the initial phase of the project provided traceability of the phenomena that describe the small-scale cyber security ecosystem. However, the main criticism of the approach is the time required to achieve theoretical saturation in the dataset in a pure application of Grounded Theory [26]. For this reason, we describe the use of the approach as a Grounded Theory *analysis*. The theoretical sampling has led to the emergence of a broad variety of themes and we are confident that the sample size is within the recommendations of Guest et al. [39] (12-20 interviews). However, the complexity of the small-scale cyber security ecosystem means that, while new themes stopped emerging in the groups our theoretical sampling led us to, there may be groups, either still emerging or entirely disconnected from the discussion, who could provide future researchers with additional themes.

3.3.2 *Case study validation*

Although we have sought peer-review for our research outcomes in line with the conventions of academic research, in Grounded Theory it is the feedback of stakeholder participants that validates the research outcomes [26].

During the course of the analysis, samples of the emerging themes were taken back to existing participants and more widely discussed with members of the three stakeholder groups present in the small-scale cyber security ecosystem. Their feedback, questions and approbation was incorporated to refine the analysis and validate results.

In some cases this information was presented in writing as email updates to participants, or, given the time constraints of the participant group, discussed informally over coffee. Alongside these less formal approaches, we formally presented summaries of our outcomes to a number of participants spanning all three stakeholder groups.

In response to feedback from our participants about the time constraints they faced when engaging with us and the mixture of definitions they gave certain key cyber security terms, the information provided for their evaluation was often provided as short 'executive summaries' with images summarising how the information provided to us had been combined with data from other participants. This is in line with approaches

Phenomenon	Concepts	Codes
Small Scale IT User Profile	SSITUs	SME
		Charity
		Individuals not connected to large stakeholder
		Families
	Other Stakeholders	Large organisations
		Individuals connected to large stakeholder
Digital Footprint	Time	Time
	Security vs Privacy	Security of the Individual
		Privacy Measures
	Cyber Footprint	Public Data
		Right to be Forgotten
		Social Media
		Footprint Consequences
Cyber Decision Making	Privacy	Privacy Erosion
		Surveillance
	Vulnerable Users	Children
		Teenagers
		Any Users
	Security Decision Making	Password Management
		Attitude to Security
		Free
		Evolution
		Good Practice
		Safety Good Practice
		Knowledge
		Training
		Security Measures
	Business Decision Making	Trust
		Cost-Benefit Analysis
		Assets
		Resource
		Need
		Business Processes
	Usability	Usable Decisions
Security Incentives	Insurance	Conditions of Insurance
	Support for Small Orgs	UK Cyber Strategy
		IT Support
		Reporting

Table 3: *Coding table summary*

Phenomenon	Concepts	Codes
Security Incentives Contd.	Risk	Supply Chain
		Data Protection
		Reputation
	Threats	Threat Intelligence
		Security Capability
Threat Incentives	Attacker Incentive	User Vulnerability
		System Vulnerability
		Inexpensive Exploitation
		Motivation
	TTPs	Opportunistic Attacks
		Targeting
Interaction/ Interconnection	Managing Interactions	Contracts
		Consumer Expectations
		Supply Chain Expectations
		Standards
		Compliance
	Cross-Organisational Communication	Information Sharing
		Reporting
		Notification
	Complexity	Complexity
	Multi-use Systems	Network
		Devices
		Credential Re-Use
		BYOD Policies
	Supply Chain	Supply Chain
Infrastructure	Infrastructure	Vendor Choice
		Mobile Devices
		Routing
	Virtual Organisations	Outsourcing
	Security Measures	Technical Measures
		Segregation
		Secure Products
		Resilience
Ownership/Control	Ownership	Data
		Identity
		Infrastructure
		Cyber Risk
		Responsibility

Phenomenon	Concepts	Codes
Ownership/Control Contd.	Support	Peers
		Government
		Professionals
		Initiatives
	Partnership	Engagement
		Roles
		Self Protection
Cyber Physical	Safety Risk	Safety Risk
	Internet of Things	Consumer CPS
		Emerging IoT
		Unused Capability

in other fields, for example design [133], and the requirements engineering process used in the second phase of this study [90].

Our method of communication with participants during the validation stage, combined with the reduced opportunities to record interviews (so that the ability to quote participants was limited), means that data fragments present in Chapters 4 & 5 are often presented in a visual format. These data fragments or analytical summaries presented to participants for discussion during the validation stage are labelled throughout the dissertation.

3.4 Generating the small-scale cyber security requirements framework

In Chapter 6 we take the knowledge provided by the UK case study — all the phenomena discussed in Chapters 4 & 5 — introducing these themes into the Volere requirements engineering (RE) process as part of the business analyst's "trawl for knowledge" [90]. The intention was to produce a requirements framework that, by enumerating constraints, requirements and security goals, could make increasing SSITUs' cyber security a more accessible problem for security providers (of any size) to address.

Although there are overlaps between different requirements engineering approaches, we aimed to produce requirements (rather than evaluate the approaches for generating requirements), leading to the decision to consistently use one widely-adopted process rather than testing our own amalgamation of different processes. The Volere RE process has been selected rather than other RE processes (for example that described by Weigers and Beatty [124]) because of its initial focus on business goals, without the assumption that *software* will be the solution. This ties in with cyber security best practices, which often emphasise the development of procedures and a focus on human factors in conjunction with the implementation of technology.

3.4.1 *Trawl for knowledge*

Robertson and Robertson define a *trawl for knowledge* as an attempt to understand 'work' as currently carried out by an organisation (or a group of customers) [90]. This exploration is intended to be technology-agnostic, describing the 'essence' of the work rather than a process' current incarnation.

The evaluation was approached using an adapted trawl for knowledge — we approach the analysis with the intention that requirements be *security solution agnostic*. In the case of cyber security best practices, this means that the "essence of the work" was evaluated independently of assumptions about existing technology and business processes. By contrast, it was not possible to be entirely technology-agnostic when drawing from our knowledge of SSITUs' operational context — their implementation of technology aids in defining key constraints that influence the development of cyber security measures. In this instance we have suspended any assumption about cyber security measures embedded in or layered over these technology choices.

3.4.2 *Engineering requirements*

In contrast with our aim to provide global requirements for a range of cyber security solutions aimed at the SSITU group, the RE process is typically used with a specific product goal in mind [124]. However, it can also be used to produce reusable requirements. In this instance the aim is to look for similarities rather than differences between projects (for our purposes, the stakeholders, environment and a goal of increasing security) so that future projects can build upon or adapt reusable requirements.

This means that the requirements have to be developed with sufficient formality and structure to make them unambiguous to other project teams [90]. In order for this to be an effective approach for developing the framework, we had to assume that framework users would be able to adopt an iterative requirements generation process — providing an opportunity to pass a quality gateway and validate the framework's global non-functional requirements before any functional requirements are developed by framework users.

A subset of RE processes are used to both structure and further abstract the survey results away from the specific examples given by project participants and towards a framework that can be applied by a variety of stakeholders. These include:

- Stakeholders and their goals.
- The "essential business case" described using context diagrams, defining scope, and with an example scenario (based on the themes developed in the earlier phase of the project), to assist in both our discussion and help framework users align the requirements we identify with the business use cases needed to identify functional requirements.
- Elements of the Volere requirements template, to provide a uniform structure to our identified requirements.

Robertson and Robertson advocate remaining technology-agnostic when defining the essential business case [90]. The scenario and related business use cases can then

Project Drivers
Project purpose — business context and project goals
Stakeholders — customer and client
Non-Functional Requirements
Ease of use, understandability and politeness requirements
Learning and training requirements
Precision or accuracy requirements
Reliability and availability requirements
Robustness and fault tolerance requirements
Capacity requirements
Scalability or extensibility requirements
Longevity requirements
Expected physical environment
Requirements for interfacing with adjacent systems
Maintenance and supportability requirements
Access, integrity and privacy requirements
Audit and documentation requirements
Immunity requirements
Cultural requirements
Compliance requirements
Standards requirements & reusable components
New problems and requirements for migration
Design Constraints
Implementation environment of the current system
Anticipated workplace environment
Customer budget constraints

Table 4: *Volere requirements types expected to be present in the requirements framework [90]*

be used to assist in the definition of a technical solution that could transition an organisation to this future desired state, although for the purposes of developing the framework this stage is out of scope.

Thus defining the framework will focus almost entirely on the definition of *non-functional* requirements and constraints.

Somerville and Sawyer describe how constraints come from the application domain, from the regulations applied to a certain business sector to a capability resulting from a specific operating environment. Constraints both generate system requirements and limit other requirements [95].

Table 4 provides a summary of all the requirement types described by Robertson and Robertson that we expected to be present in our requirements framework.

3.4.3 *Requirement validation*

Robertson and Robertson describe how a gap analysis type approach — working uniquely with a present and anticipated future state — is too simple, and so "unsuitable for any kind of serious innovation" [90]. As such, we have avoided using examples of specific SSITU cyber security solutions as a way of validating the requirements framework, instead focusing on the validation processes present in the iterative RE process itself.

In [90] Robertson and Robertson describe the requirements validation process in two parts. These processes are designed to test the *accuracy and completeness* of a requirements specification, the authors highlighting how *requirements exist irrespective of our ability to elicit them.* In the context of this project, knowledge of a requirement's existence comes from the trawl for knowledge (completed using rigorous qualitative methods), thus this validation tests *only* our ability to translate these research outcomes into usable requirements:

- *For individual requirements* — a quality gateway was used to test if a requirement is 'acceptable'. The gateway incrementally defends the finalised requirements specification against incorrect requirements, reducing the cost of mistakes. It tests requirements for scope, relevancy (to both small organisations and the essence of cyber security best practices), completeness, ambiguity, consistent terminology, viability within constraints and to ensure they are not solution-bound.

- *For the requirements specification* — the specification was reviewed for completeness, taking into account whether the requirement types expected (Table 4) are present and whether the use cases have been identified and subsequently satisfied.

Once the requirements specification had been defined there were two further factors that influenced the content of the requirements framework. There are always too many requirements, leading requirements engineering processes to include an element of prioritisation. For example, Gilb suggests that key requirements — those which have the greatest impact on key stakeholder values and system constraints — should be identified and that other, non-essential, requirements can be discounted during the design process [36]. Robertson and Robertson suggest prioritisation take into account the cost of implementation, the value to the customer, the time and ease of implementation of both technical and business measures, the benefit to the organisation, and finally legal requirements [90]. All requirements in the framework have a priority level: critical (C), important (I), and optional (O). We have had to further prioritise when choosing the requirements that we discuss in Chapter 6, summarising and referencing some of the framework's requirements, which can be found in full in Appendix D.

The other factor to influence the final description of the requirements framework is the conflict of requirements. In the context of this dissertation the number of constraints will severely limit stakeholders' abilities to prioritise certain types of requirement.

Table 5 describes the attributes present in the requirements presented in Chapter 6 and Appendix D. Constraints identified during the trawl for knowledge will take the same structure, but instead of being given a priority level, will be flagged as unchangeable (X). In some cases constraints will not have a fit criteria — many con-

Attribute	Description
Requirement ID	*Unique identifier*
Requirement Type	*Type as defined in Table 4*
Description	*Intention of the requirement*
Rationale	*Justification — tied back to knowledge and scope*
Source	*Described by which stakeholder group*
Fit	*Proposed measure to test solutions against requirement*
Priority	*Rate value/importance to the customer*
Conflicts	*Requirements that can't be implemented in combination with this requirement*

Table 5: *Requirement structure (driven by [90])*

straints describe the operating environment and influence other requirements, without describing a design requirement in their own right.

3.5 VALIDITY

The ideal would have been for the researcher to begin the project with complete objectivity about the subject of the study; however, researchers always have a certain amount of influence over the project outcomes. In order to better define the role of the researcher in the theory-generating process, the subject of *reflexivity* has been developed [26].

Stier, in referring to reflexivity, states that *"the research process itself must be seen as socially constructing a world of worlds with researchers included in, rather than outside"* [96]. He suggests that there is a usefulness in self-reflexivity to help us in understanding what others are doing. The concepts of reflexivity and the need for as many viewpoints as possible is mirrored in the requirements engineering process — analysts need to avoid starting with the assumption that they already know all of the requirements [37]. Robertson and Robertson also state that an analyst often needs to be present in the research asking the correct questions to *elicit* requirements where the customer may not be entirely sure what they want — "in order to complete the requirements elicitation process, sometimes the business analyst has to be more than a stenographer" [90].

The difficulties in balancing the use of self-reflexivity was highlighted in the preliminary study, where the phenomena of a lack of engagement from small-scale IT users and high investment in the development of security measures for large organisations were identified. Varied viewpoints during the requirements engineering process had been replaced by reflexivity in the design process and the re-branding/adaptation of security measures designed for larger organisations for small-scale IT users. This outcome highlighted how the success of the project hinged on having a breadth of perspectives in the sample group.

Corbin and Strauss suggest thinking comparatively to stay grounded in the data and maintain distance and objectivity [26]. The need for comparative thinking during data analysis has to some extent driven the scope of the project, ensuring that there are sufficient points of view in the data. Participants were selected using theoretical, rather than random, sampling, meaning that alternative viewpoints were gained by sampling according to emerging concepts during analysis [26]. The initial outline of incumbent

models such as large corporate cyber security, safety and privacy also provides an existing framework for comparison when evaluating the cyber security needs of small-scale IT users against other common practices.

The success criterion of a Grounded Theory project is typically the extent to which the research outcome fits with the data used to generate it — in the context of the dataset does the result make sense [26]? The outcomes of the requirements elicitation process have been recorded in a format which is auditable by: the validation process described in Section 3.4; academic peer review; and each time the framework is adopted in the development of products aimed at SSITUs. The accuracy of each requirement in relation to a specific project (and the likely reusability of the model as a whole) can thus be measured over time.

Sampling for the questionnaire dataset highlighted some skew in the sample due to SME participants needing to have an interest in cyber security (and so some basic awareness) in order to make time to participate. The interviews continued to use the UK as a case study when sampling the stakeholder group. These skews will limit the applicability of the framework — it won't tell risk-holding stakeholders how to engage completely disinterested SSITUs in cyber security, but it will help them develop advice that is adapted to the target users. There is also likely to be differences internationally in the way small organisations operate and so the decisions they make — while the financial constraints caused by a lack of economies of scale will exist in all small organisations, other constraining processes or decisions may be culturally specific.

During the interviews the participant group was broadened to include non-SME stakeholders who could provide insight into the dialogue on cyber security from alternative perspectives. Many of these are from UK Government bodies (where the cyber security community is relatively small), who often have a liaison dedicated to external communication about cyber security. Identifying these liaisons often requires introductions via contacts in other government bodies, inevitably leading to a number of the risk-holding or security-providing participants knowing at least one other participant. Participants in the different small-scale IT user groups were contacted independently via social networks or contacts within the University of Oxford, with an intentional overlap (n=2) with the initial questionnaire data to calibrate the two datasets against each other.

3.6 SUMMARY

This chapter described and justified the use of Grounded Theory and Requirements Engineering in our research design. Based on these two approaches we have outlined the methodology used, which provides the approach for both eliciting phenomena and requirements from the small-scale cyber security stakeholder group and a means of validating those outcomes.

4

RISK AND THE SMALL-SCALE CYBER SECURITY DECISION MAKING DIALOGUE

Our initial study highlighted how *security* experts' assumptions that the cyber security 'best' practices described in Chapter 2 are scalable to small organisations acted as a barrier to entry for *small business* experts/owners [76]. 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 chapter we focus on decision making and risk assessment (RA) practices within SSITUs, comparing the processes implemented with common corporate cyber security practices.

Following on from the context provided by Chapters 1 and 2, this chapter uses the outcomes of the empirical study described in Chapter 3 to generate the first half of our UK case study, by framing a response to the following research question: *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. In Section 4.1 we discuss how (irrespective of risks or their mitigations) the context within which SSITUs operate alters their decision-making priorities. In Section 4.2 we use a realistic 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 4.3 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 threat landscape and introducing issues of influence into the discussion of SSITUs' ability to treat risk. As such, Section 4.4 discusses incentives for risk-holding stakeholders to secure the supply chain. We summarise the outcomes of the chapter in Section 4.5.

This chapter is based on [75] and is discussed as Contribution Chapter 1 in Chapter 1. A table of the phenomena and concepts explored in this chapter can be found in Table 6.

4.1 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.

Phenomenon	Concepts
Cyber Decision Making	Privacy
	Vulnerable Users
	Security Decision Making
	Business Decision Making
	Usability
Threat Incentives	Attacker Incentive
	TTPs
Security Incentives	Insurance
	Support for Small Orgs
	Risk
	Threats
Ownership/Control	Ownership
	Partnership

Table 6: *Phenomena and concepts explored in this chapter*

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.

4.1.1 *Business decision making*

As we saw in Chapter 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. [129] 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. Pfleeger and Pfleeger suggest that all decision makers have to balance the security decisions they make with other activities that need investment [80]; however, the combination of resource constraint and lack of influence increases contention in decisions made by the SSITU group.

4.1.1.1 *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 [52] 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.

4.1.1.2 *System complexity*

Our data indicated that complexity also has a role to play in decision making. In large organisations the decision makers have responsibility for both higher budgets and risks — Blau indicates that the complexity is proportionate to the organisation but the decision makers are usually specialised in the area they have responsibility for [17].

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? (This question is discussed in detail in Chapter 5.)

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 risk-holding (RH) stakeholder entering into an agreement with a SSITU.

4.1.2 *Resource constraint*

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

4.1.2.1 *Human resources*

SSITUs have a limited number of employees, but still need to carry out activities similar to those carried out by large organisations. Blau notes a difference in the lack of specialisation [17], which our data replicates: 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. [129], 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 4.1.3.

4.1.2.2 *Cyber security budgets*

Some of the issues discussed in this section are inherent to small organisations; however, small organisations in our dataset are clearly doing a cost-benefit analysis in implementing their security measures, in line with good practice [80]. 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.

In our initial study SMEs were asked how much they currently spend on cyber security [76]. The responses can be seen in Figure 9, with additional detail provided by Figure 10. Quantified budgets from the questionnaire dataset, combined with discussion in subsequent interviews, highlighted three factors RH and security-providing (SP) stakeholders may wish to be aware of:

1. As would be expected, the budget a company is willing to allocate on cyber security increases with the size of the company (Figure 9).

2. It was possible to estimate a cyber security budget as a per-person value (Figure 10). Micro-companies invested £10-50 per person per year. Small companies (10-49 people) either followed the same pattern of investment as micro-

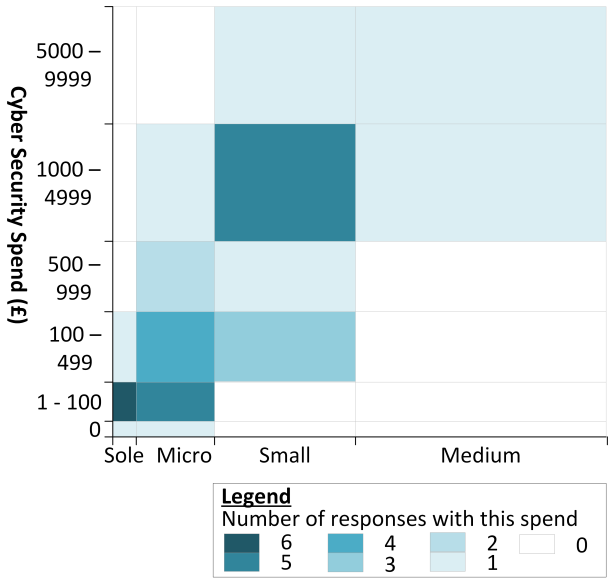


Figure 9: *Data fragment discussing cyber security budgets: cyber security spend in SMEs by size from questionnaire responses*

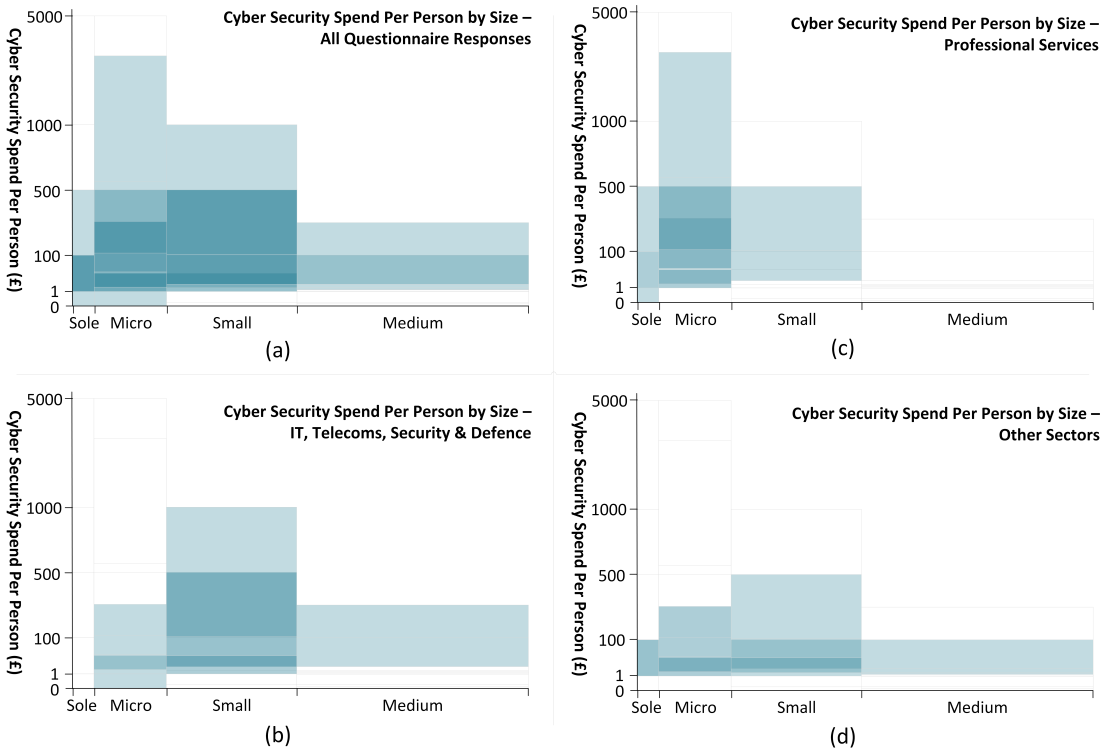


Figure 10: *Sample of data analysis showing cyber security budgets per person in SME questionnaire responses: (a) all questionnaire responses; (b)–(d) by sector*

companies, or 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. This difference in investment can be seen most clearly in Figure 10(b), where two separate business cases emerged, differentiating between financing cyber security as a business process and financing a saleable capability or professional reputation.

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.

4.1.2.3 *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.

4.1.3 *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.

4.1.3.1 *Security awareness*

As stated in Chapter 2, concern over the level of cyber security awareness came mainly from the RH and SP stakeholder groups. One participant stated that advice 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 [86], 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 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.

4.1.3.2 *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[1] — and Lazear [51] 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. We observed a link between participants having no security expertise and their confidence that they could apply suitable measures, indicating either complacency or the entrepreneur's typical reaction to a challenge. As discussed in Chapter 2 Renaud agrees with this hypothesis, highlighting how SME decision makers need to see a realistic chance of managing a threat to attempt its reduction. Rhee et al. [87] suggest that confidence encourages security adoption, whereas the stress of an incident reduces self-efficacy. Van Eeten and Bauer [118] 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 [27] 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.

1 www.dictionary.com/browse/entrepreneur

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. Subashini and Kavitha suggest that many of these easy-to-use services make privacy and confidentiality by default difficult [99] and this is being mirrored by the description of SSITUs' ability to own and control their systems in our analysis. 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' [129], 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.

4.1.3.3 *Peer-support*

There is a scarcity of cyber security experts[2], and this influences how affordable their skills are for SSITUs. Participants highlighted how government accreditations such as Cyber Essentials Plus [111] 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 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.

4.1.3.4 *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

2 www.ft.com/content/4cabd0fe-8940-11e5-90de-f44762bf9896

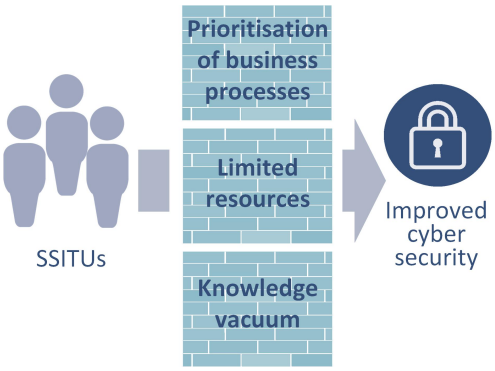


Figure 11: *A summary of the contextual barriers to the implementation of cyber security that emerged from our analysis*

automated systems that allow them to increase security without needing to gain 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 is 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.

Before considering security investment, there are a number of barriers for SSITUs to overcome; this is summarised in Figure 11. 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.

4.2 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 4.1, 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 a more lightweight process 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 4.2.4–4.2.6). Finally, in Section 4.2.7 we discuss the risks faced by those SSITUs identified in Section 4.2.1 as not needing the risk assessment process.

4.2.1 *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, mak-

ing 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 on a risk-based strategy, moving a no-security system towards a perceived benchmark.

4.2.2 *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.

4.2.3 *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 ISP. These networks are shared with other members of the employees' households.

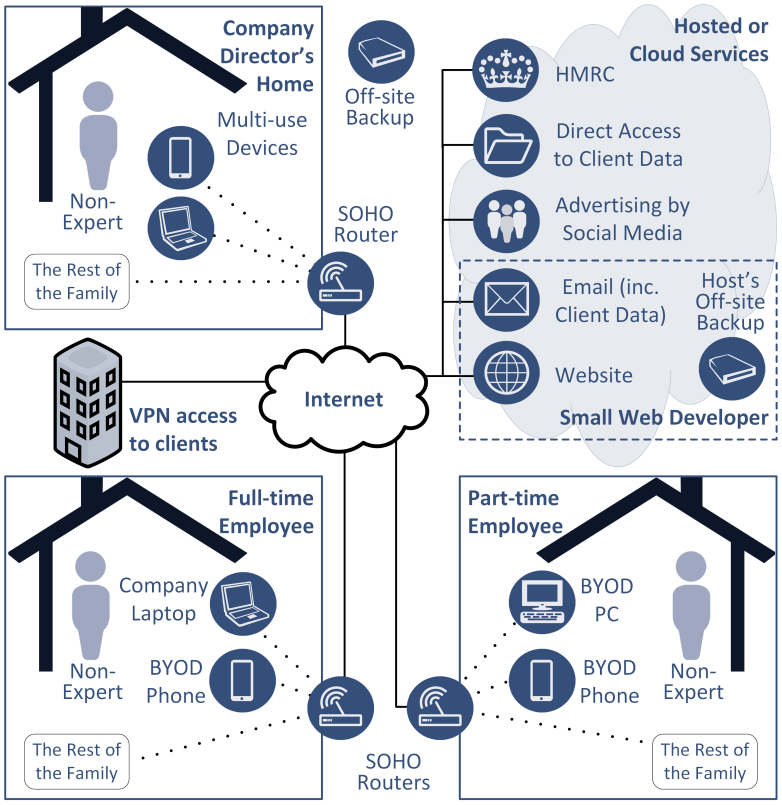


Figure 12: *Scenario architecture*

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 12.

4.2.4 *Scoping and engagement*

4.2.4.1 *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 — Alberts and Dorofee suggest that the inclusion of multiple members of staff introduces a need to discuss requirements, increasing the breadth of risks identified [13].

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

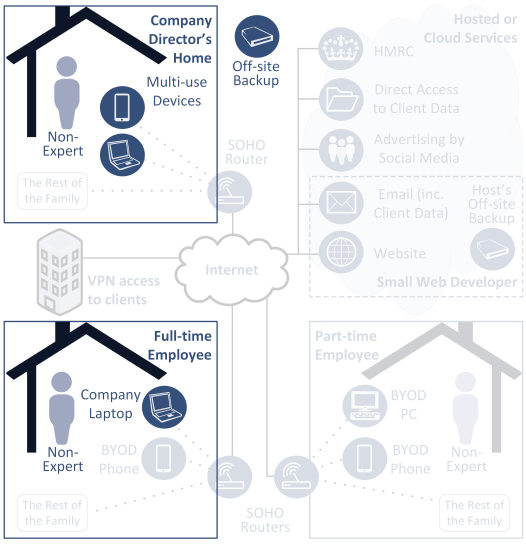


Figure 13: *Decision-maker controlled elements of the scenario archiecture*

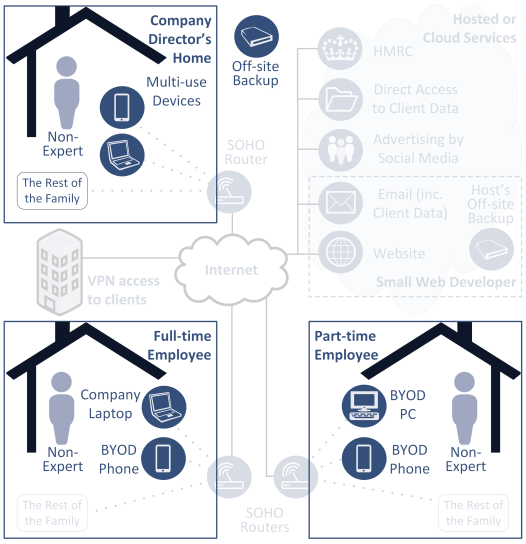


Figure 14: *Decision-maker and IT policy controlled elements*

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.

4.2.4.2 *Defining a meaningful scope*

Pfleeger and Pfleeger describe the aim of carrying out a RA as one of identifying and prioritising risks for treatment so that an organisation can achieve the most security for their investment [80]. 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 13. 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 14, it does not increase the scope to include the web developer due to the lack of knowledge described in Section 4.1. 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 12.

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, which Berger and Jones suggest are possible in SMEs [16], can be carried out only where a system owner has given permission [38]. 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 [99] 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 [46] — 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. [46] 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 [46]. 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 4.4).

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 [118] 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*[3]), 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 ex-

3 ec.europa.eu/DocsRoom/documents/4942

tent 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 knowledge (as described in Section 4.1), which could limit the extent to which SSITUs are able to select a scope based on an understanding of threats (discussed in detail in Section 4.2.5), or the potential breach impact that the decision maker believes the company faces.

4.2.5 *Identifying threats*

In their qualitative risk assessment process Alberts and Dorofee suggest identifying cyber security threats to critical assets [13].

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 4.2.5.1–4.2.5.7 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.

4.2.5.1 *The availability of threat intelligence for SSITUs*

Data feeds about threats faced in certain sectors are available from CERT[4]. 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[5].

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[6]). 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[7]) 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.

4 www.cert.gov.uk
5 Information Commissioner's Office: Action we've taken: ico.org.uk/action-weve-taken
6 www.ncsc.gov.uk/cisp
7 www.openioc.org

This brings us back to the problems faced by SSITUs when searching for free security advice described in Section 4.1: SSITUs need to understand the cyber risks relevant to their systems, but also the risks that different post-incident actions might represent.

4.2.5.2 *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 [13]. 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* — for example, Pfleeger and Pfleeger describe a scenario where the owner has a potential for financial loss, and/or an attacker has something to gain [80]. 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."

$(ISC)^2$ train cyber security professionals that 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 [38]. This is where SSITUs in this study had the greatest 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 4.1 about resources and ability, and how advice is muddied by inconsistency [86].

Throughout this chapter 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.

4.2.5.3 *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." [55]

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, for example from Scott-Railton [92].

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 4.2.5.4 and 4.2.5.5 discuss the different assets an attacker may be focussing on when attacking a system.

4.2.5.4 *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.

Subashini and Kavitha suggest that the value of data is a function of its quality [99]. 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). However, the interpretation of this type of threat by our SSITU participants was incomplete, only measuring value that they perceive.

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[8].

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.

4.2.5.5 *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[9] — 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.

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

9 www.team-cymru.com/ReadingRoom/Whitepapers/TeamCymruSOHOPharming.pdf

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.

4.2.5.6 *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.

Lusthaus describes how vulnerabilities can 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 [57] — this suggests that 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.

4.2.5.7 *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, for example [68]. 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 4.1. 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 4.1 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 [86]. 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 15. 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 4.1, 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 [13] 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 4.1 make *all* threats, from script kiddies to well-resourced knowledgeable actors, more difficult to repel.

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.

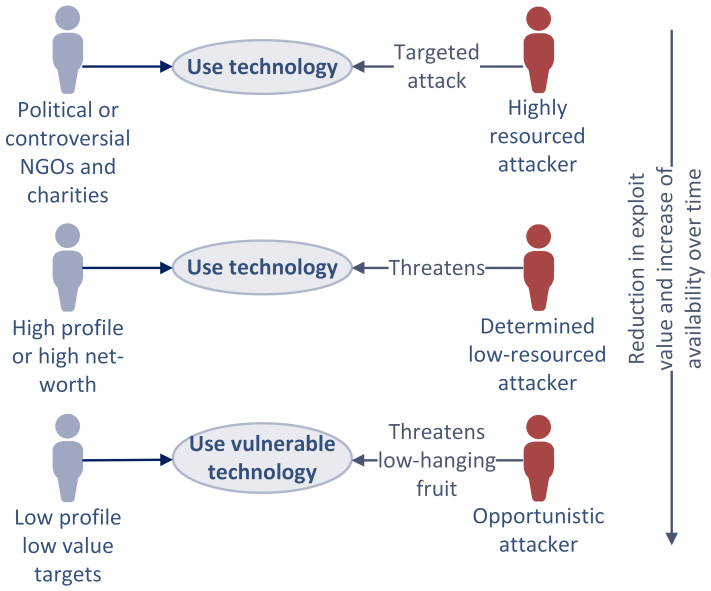


Figure 15: *Sample of analysis presented to participants for validation: misuse cases concerning different SSITU groups*

4.2.6 *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.

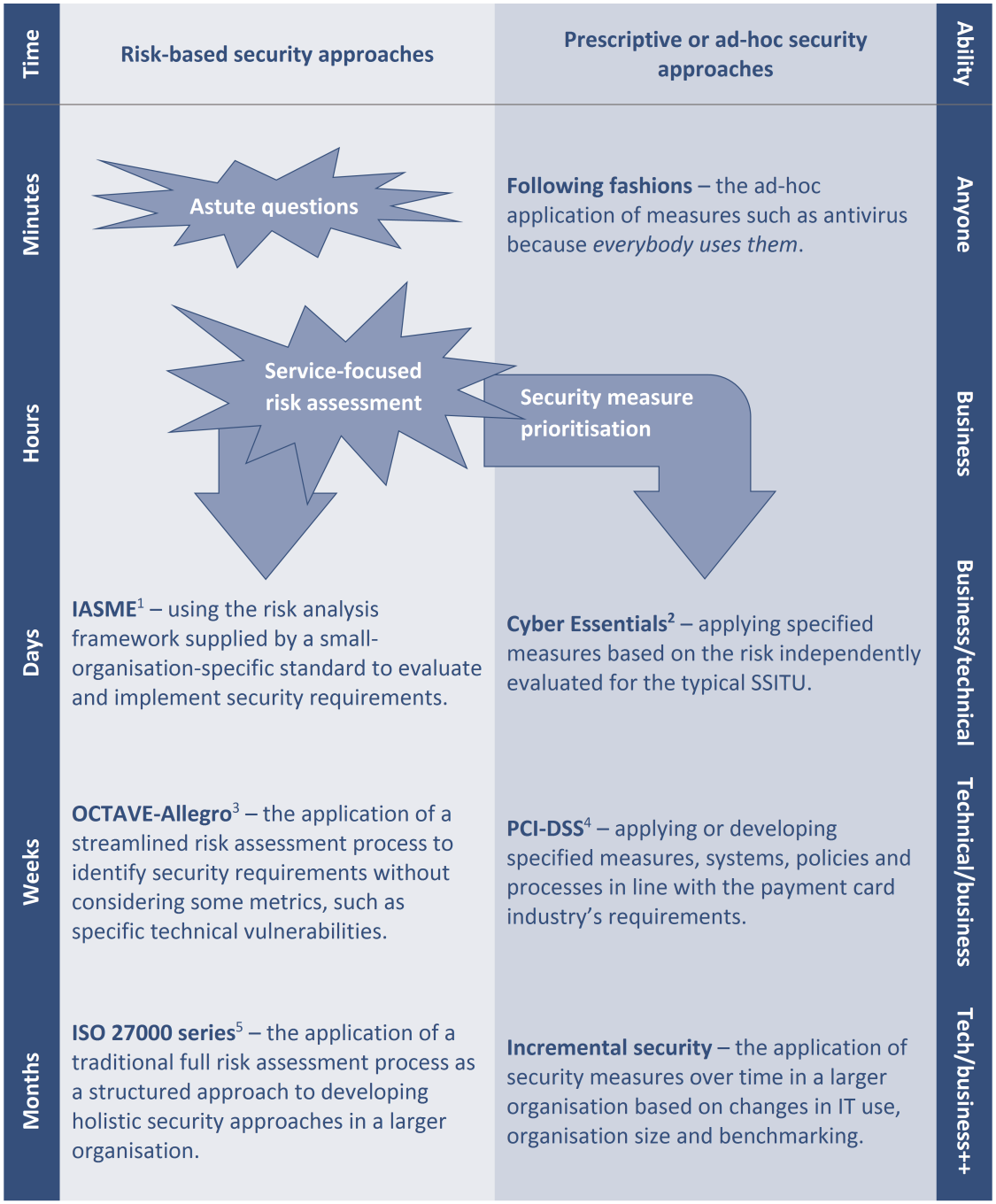
In Section 4.2.4 we discussed how system control influences the scope chosen for a RA. There were obvious control constraints for the SSITUs who participated in our study, although virtual organisations are those who have the greatest issues, by not owning any of the devices or networks through which 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.

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 16.

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



[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 16: *A summary giving examples of the gaps in entry-level options for organisations to increase cyber security used for triangulation from SPs to SMEs*

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[10] 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 4.2.3 was by no means a worst case scenario for risk in the SSITU group. We identified two types of *high risk SSITU* based on comments made by our participants:

1. The charities or public figures mentioned in Section 4.2.5 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 4.1 — resource or knowledge — being overridden by regulation in cyber security.

4.2.7 *Risk for other SSITUs*

As outlined in Section 4.2.1, a proportion of our SSITUs will never feel the need to assess their risk, making analyses such as those carried out in Sections 4.2.4–4.2.6 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

10 www.iasme.co.uk

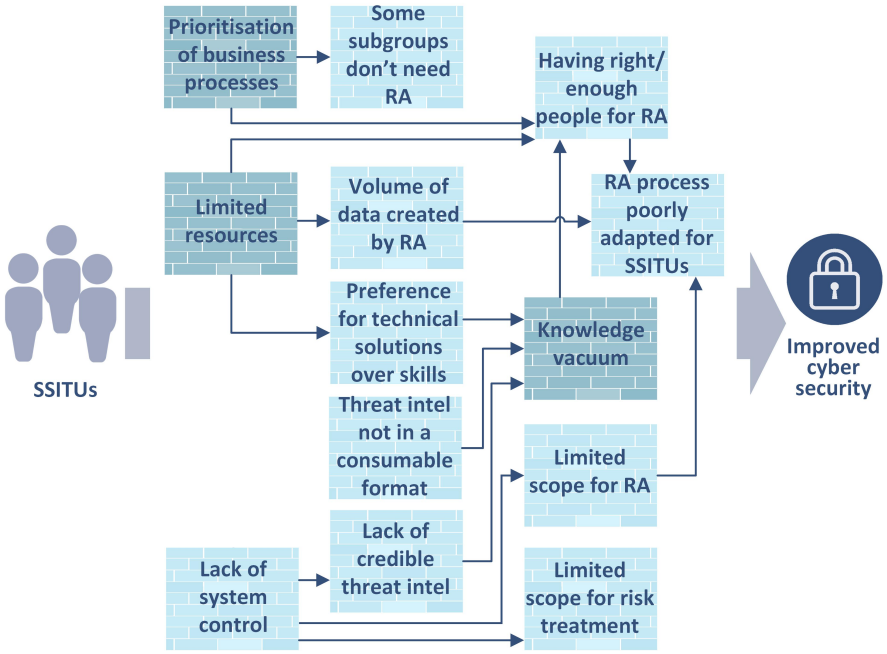


Figure 17: *A summary of the contextual and procedural barriers to the implementation of cyber security that emerged from our analysis*

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 4.4).

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 17 expands on the contextual barriers described in Section 4.1 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.

4.3 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 applicable only to a subset of SSITUs (as described in Section 4.2).

4.3.1 *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.

4.3.2 *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 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'.

4.3.3 *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 a questionable commitment to security processes that might protect it, "reputation is everything" to small organisations. As mentioned in Section 4.2.5, 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 [68]. 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.

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.

4.3.4 *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 18 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 17, 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.

4.4 Security incentives and disincentives for risk-holding stakeholders

The high level of interactions in the supply chain described in Section 4.2 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 stakeholder group are summarised by the misuse cases illustrated in Figure 19.

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.

4.4.1 *Concerns about SSITUs' security from risk-holding stakeholders*

In Section 4.2 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[11] — suggesting either that the problem is being down-played, or that the subset of SMEs

11 www.cyberaware.gov.uk/sites/cyberstreetwise/files/cyber_streetwise_kpmg_-_small_business_reputation_report_final.pdf

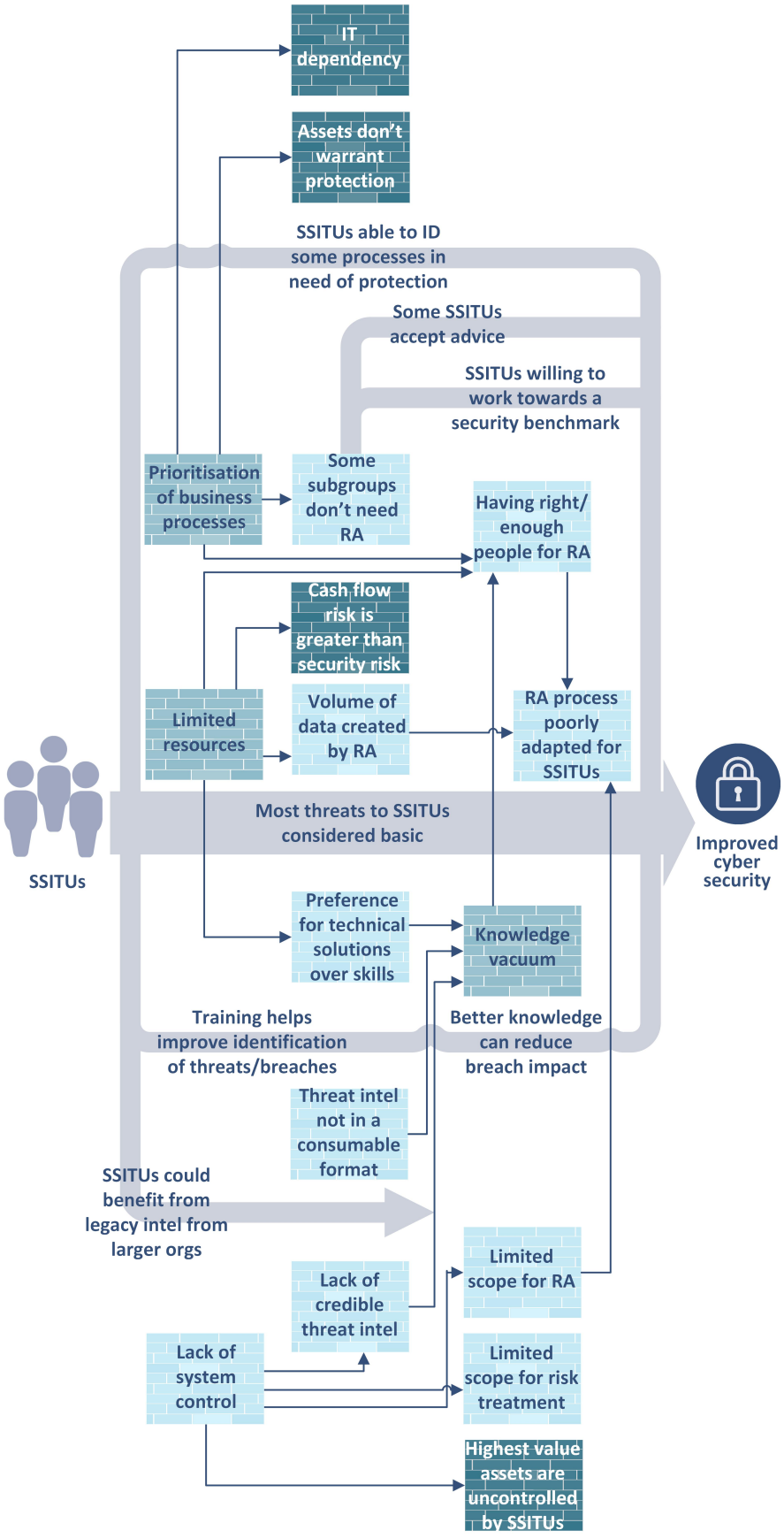


Figure 18: *A summary of the emerging incentives that circumvent barriers to the implementation of cyber security from our analysis*

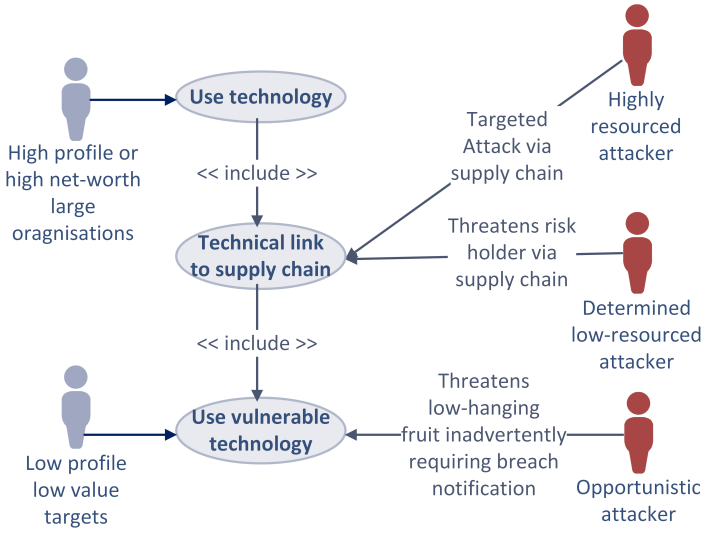


Figure 19: *Misuse cases concerning the supply chain used for a triangulation of research outcomes by our participants*

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 [46]; 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.

4.4.2 *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 risk that this poses to the economic stability of the UK led to SSITUs' inclusion in the National Cyber Security Strategy, as described in Chapter 1.

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

The sheer number 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.

Awareness of a risk could in itself act as an incentive to improve security — foreseeing the embarrassment of falling victim to an attack, combined with an awareness that the SSITU (as an uninsured RH) would have to absorb the costs of any successful attack, might increase the perceived 'cost' of a breach. 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[12].

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 [118] 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

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

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 [46] — 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 4.2.6.

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 4.1 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 chapter (Figure 20), which shows, despite the many barriers identified by our SSITU participants that there are still pathways for improving SSITU security. In the case of SMEs, our data suggests that 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.

4.4.3 *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 4.2, 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 Section 4.4, 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 on the Internet. Scare stories"

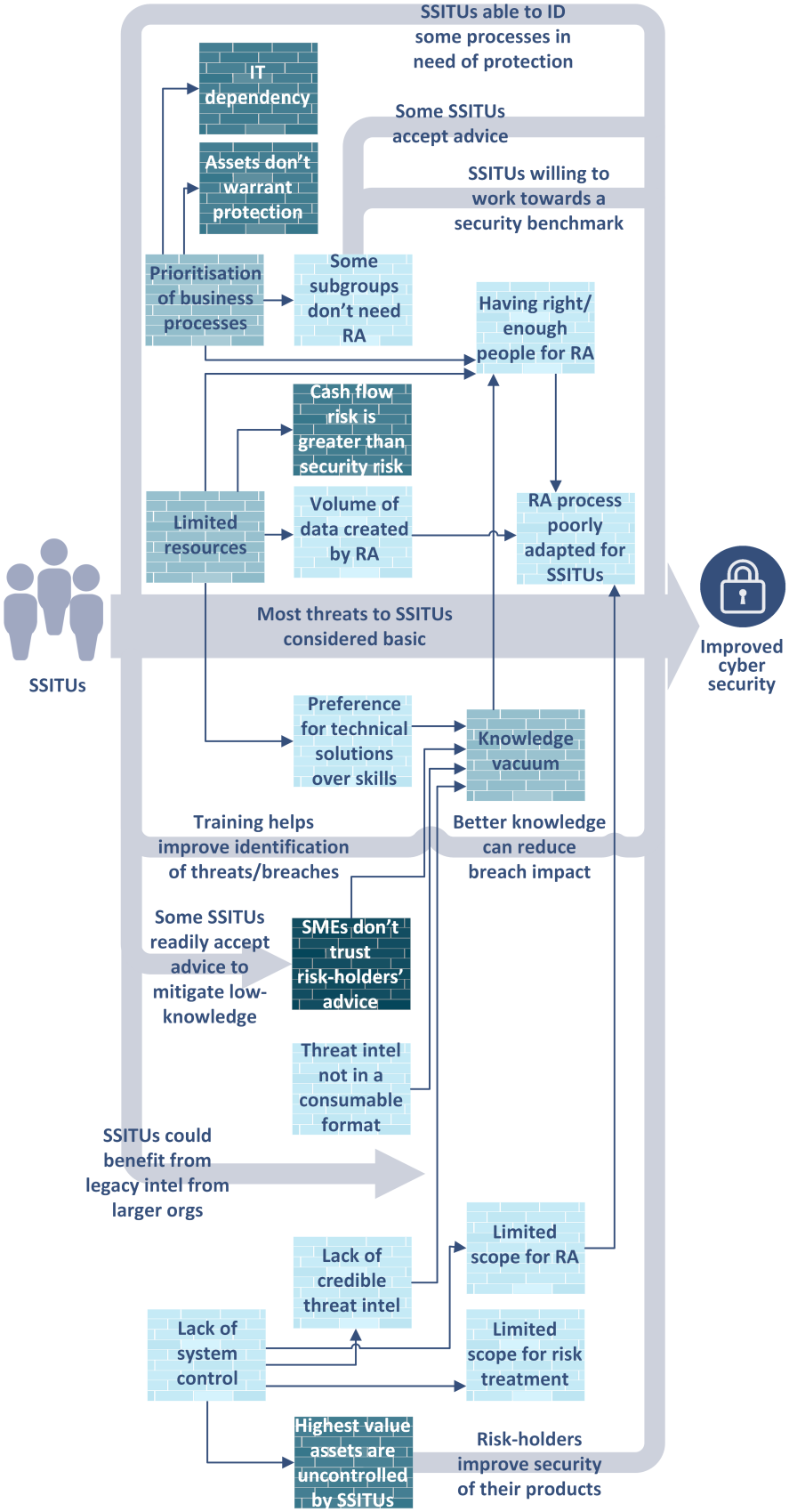


Figure 20: *A final overview showing the interation of barriers to cyber security decision making and incentives to secure, including the impact of RH stakeholders, as emerged from our analysis*

- "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 [86], 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 discussed in Chapter 2 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 — as Wynarczyk et. al. suggest, unable to greatly influence suppliers or customers [129] — our analysis suggests that, 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.

4.5 SUMMARY

In this chapter we have evaluated the differences between small-scale IT users (SSITUs) and larger government or corporate entities highlighted by our survey. We have illustrated the difficulties and constraints a SSITU faces in justifying the implementation of security. Namely that:

- SSITUs *and standards aimed at SSITUs* [111] 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, make their outcomes less meaningful and make it difficult for smaller organisations to comply with the expected data protection processes.
- Very few SSITUs face more than basic threats to their own assets, 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 chapter, 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, our datasets having provided some useful challenges to some of the common assumptions made by cyber security experts. 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.

Of course, justifying the investment is only half of the cyber security challenge faced by any organisation. The following chapter presents the second half of our UK case study on small-scale cyber security, evaluating how existing IT systems, digital footprints and a lack of influence within the supply chain alter SSITUs' abilities to implement cyber security measures.

5

SMALL-SCALE IT USERS' INFRASTRUCTURE AND THE APPLICATION OF CYBER SECURITY

As stated in Chapter 1, despite ongoing government investment, private sector initiatives and increases in academic funding, the UK's 2016 report on the National Cyber Security Strategy stated that smaller businesses' *"awareness of the personal relevance of the cyber risk is patchy"* [116]. Individual consumers have shown an increased awareness of security, yet small organisations, also treated as consumers by their service providers, are lagging behind in their uptake of security advice.

In Chapter 4 we began describing our UK case study of small-scale cyber security by exploring how justifying investments in cyber security may be challenging for SSITUs. However, attempts to increase the level of cyber security awareness in small organisations has not resulted in mitigated risks. This chapter evaluates the complementary issue of operational constraints by addressing the research question: *Once a SSITU has justified investing in cyber security, what constraints within their IT system limit their decisions?* To this end, the chapter focuses on system and cyber security infrastructure, drawing comparisons between the systems implemented and common corporate cyber security practices.

The structure of the remainder of the chapter is as follows. Alongside the infrastructure (Section 5.1), an evaluation of security in emerging cyber physical systems (Section 5.2) and system interactions (Section 5.4) that make up a typical cyber security discussion, in Section 5.3 we have included the digital footprint of a SSITU — the scope of their virtual presence — as a vital element of the decision making process. We summarise the chapter in Section 5.5.

This chapter is based on [73], with research from [72] in Section 5.2. A table of the phenomena and concepts explored in this chapter can be found in Table 7.

5.1 INFRASTRUCTURE USING SMALL-SCALE CYBER SECURITY

With regards to 'good practice', cyber security includes many non-technical processes, including risk assessment, operations and secure development practices, for example, those presented by $(ISC)^2$ [38]. Yet technical solutions typically constitute the main focus of our SSITU participants' approach to security. These technical measures could be seen as an addition to, or an interpretation of, the system architecture employed by a decision maker.

Technical elements of cyber security 'good practice' vary. Despite the swift evolution of both technology and threats (and, consequently, the cyber security needs of companies), the core concepts of cyber security are relatively mature. For example, in 1987 Carroll presented *20 principles of conventional security* [21], the majority of which are still present in one form or another in contemporary standards and professional training (see, for example, [38] and [3]).

Phenomenon	Concepts
Infrastructure	Infrastructure
	Virtual Organisations
	Security Measures
Cyber Physical	Safety Risk
	Internet of Things
Digital Footprint	Time
	Security vs Privacy
	Cyber Footprint
Interaction/Interconnection	Managing Interactions
	Cross-organisational Communication
	Complexity
	Multi-use Systems
	Supply Chain
Ownership/Control	Ownership
	Support
	Partnership

Table 7: *Phenomena and concepts explored in this chapter*

Relatedly, there are a number of cyber security practices relevant to our SSITUs as they consider their systems, conveniently described to the lay person by Carroll 30 years ago [21]:

- Identify assets deserving protection
- Concentrate your valuable assets so they can be protected
- Establish your defined perimeters around your protected assets
- Defend your protection perimeters
- Maintain surveillance over your protected assets
- Control access to protected assets

In order to build context for our discussion of emerging themes around the application of cyber security, we asked both questionnaire and interview participants to tell us about the type of IT they used, as well as the implementation of security they implemented.

As we will depict in the remainder of this section, some of the most limiting constraints SSITUs face when implementing security measures are related to their distributed digital assets, the difficulty they have in defining a perimeter, and the shared nature of much of their infrastructure.

Our survey has indicated that infrastructures used by SSITUs can be differentiated from large corporate IT systems in a number of ways: in terms of organisation size, organisation maturity, and organisational mission and IT strategy.

This section discusses these differentiators and the impact they may have on the application of cyber security by SSITUs. The organisational differentiators all result in

Type	Total
Home users	13
Single person companies	11
Micro-companies	18
Small and medium-sized companies	15
Mature organisations	5
High infrastructure or large organisations	5
Low infrastructure organisations	20
Virtual organisations	2
Multi-purpose infrastructures	14

Table 8: *Participant statistics — the number of participants reporting on each type of organisation infrastructure.*

SSITUs implementing slightly different infrastructure, with Sections 5.1.1–5.1.3 exploring the resulting IT infrastructure each type of SSITU maintains (this is complemented by a discussion on the virtual element of SSITU infrastructure — the digital footprint — in Section 5.3). Table 8 illustrates how our participants divide into the (non mutually-exclusive) groups the differentiators create.

All participants recognised that resources are needed to create the most secure configuration possible for their size of network, with a significant proportion of those resources pertaining to security implementation. Comments focussed on implementation, rather than the purchase of pre-configured products, reinforce the comments made by Herley [42] and highlight the issues around time and knowledge constraints in small organisations.

There was a very strong reliance from SSITUs on the embedded security in each device they purchase, partly due to knowledge and partly because of limited resource. This is particularly evident with mobile devices, which our small organisations seemed to rely upon far more than larger organisations would, especially in cases in which a SSITU does not maintain an office. Total reliance on embedded security is a concern, for example, given the financial outlay required to purchase mobile devices combined with manufacturers' tendencies to customise operating systems, then cease to generate updates, commented on by [104].

The security measures adopted by SSITUs can be categorised using the terminology employed by various participants:

- *Basic measures* — that every participant employed, whether or not they understood what the measure would achieve, including operating system patches and antivirus.
- *Reactive measures* — measures implemented as a result of a security incident, such as increased redundancy or reactive patching.
- *Proactive measures* — measures applied to reduce an identified risk.
- *Measures for resilience* — including disaster recovery planning, backups and system redundancy.

5.1.1 *Infrastructure by size*

In defining how *small-scale* IT users apply cyber security, the first characteristic we explored was organisational size. It was this examination in the SME user group that led to our broader definition of SSITUs, as the smallest of these organisations have a significant overlap with topography of home networks and an increase in the intersection of different user roles within a single system.

Although it would be impossible to define what a single 'normal' SSITU system architecture could look like, we have identified some commonalities in IT use described by our participants and identified significant infrastructure differences dependent on organisational size.

When discussing our findings with stakeholders for the purpose of triangulation, we used diagrams representing the infrastructure participants had described to aid in identifying anomalies in our understanding of the way these organisations used IT. Led by the results of Chapter 4 — the lack of knowledge held within the SSITU group — these were presented as extremely high-level network diagrams where infrastructure was assumed to connect using service providers' default settings. Only a subset of cyber security professionals with a technical focus described attempting to circumvent default settings in a SSITU's system, while attempting to make their own home networks more secure.

5.1.1.1 *Home infrastructure*

The smallest of the SSITUs are individuals, in small home networks. At this stage the dataset already provides two distinct infrastructures: the 'typical' home network described by families, single person companies, etc. and home networks used by individuals in large-scale shared accommodation such as student halls of residence. One of our participants lived in student halls; the other 12 participants who discussed their home networks lived alone or with family.

The first infrastructure, an example of which can be found in Figure 21(a), is typified by a Small or Home Office (SOHO) router supplied by the user's ISP providing connectivity to a variety of consumer devices including laptops, PCs, smartphones, games consoles, TVs and other appliances. Networked storage, etc. is occasionally mentioned, but most storage and services used by devices in the network are cloud hosted.

There is a difference in the system setup described by participants who were knowledgeable about security, with the ability to do some additional configuration, and those who had limited knowledge using default settings. The biggest differences are listed below.

- The use of a second user-owned and user-controlled SOHO router, for improved security and to avoid the ISP having total freedom to reset any perimeter security configurations.
- The use of wired connections for the laptops/PCs the users felt needed the most security (often devices used for work purposes).
- The introduction of a demilitarised zone (DMZ) between the two SOHO routers, bypassing security because many consumer devices had rigid configurations that were incompatible with Network Address Translation (NAT).

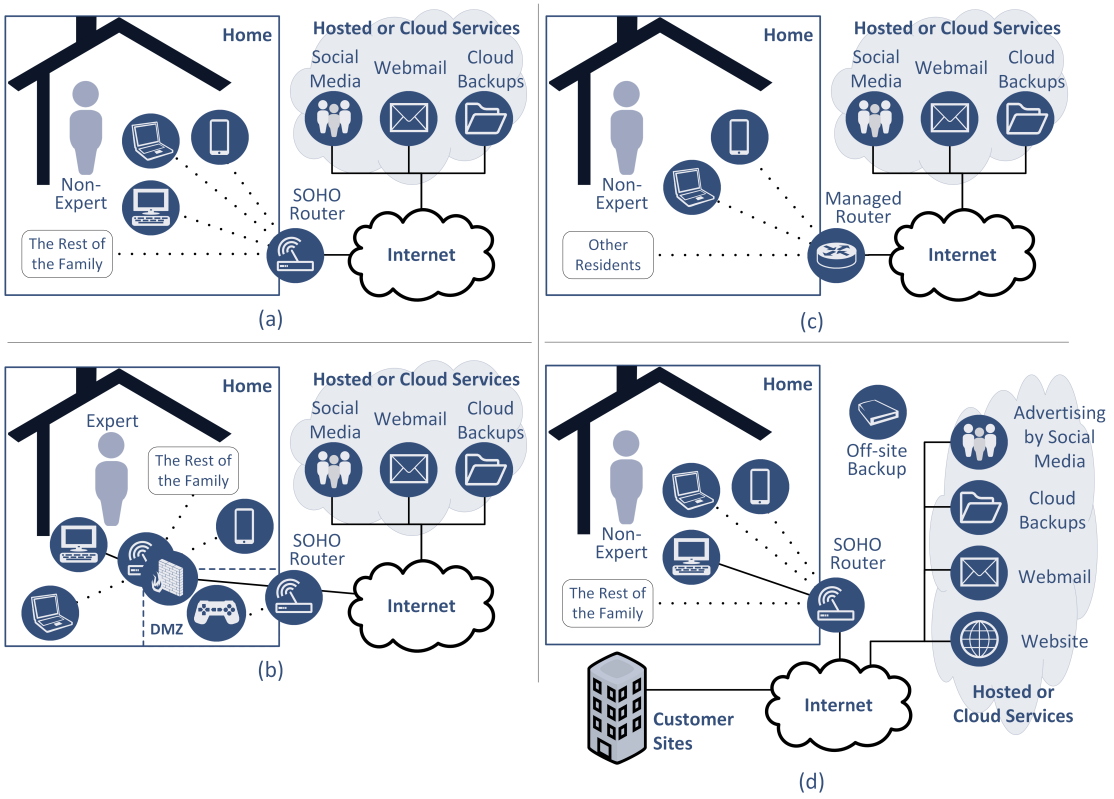


Figure 21: *Fragments of data analysis used to discuss results with participants: examples of home infrastructures using service provider default settings (a, c, d — from both the questionnaire and interviews) and a contrasting example from security professionals (b — from our interviews), who described how their attempts to add additional security were sometimes thwarted by the inflexibility of default configurations*

- The introduction of a network firewall in addition to the endpoint security found in the typical network.

For comparison, this higher security home network can be seen in Figure 21(b).

The second type of home infrastructure, for example Figure 21(c), is the IT configuration from this study over which the user has the least control. These types of system are entirely controlled by building management, who provide the same unsegregated Bring Your Own Device (BYOD) network to all tenants and their visitors.

In the case of university-owned accommodation, these BYOD networks are likely to be an extension of a corporate network. This replaces the user's ability to implement more than endpoint security with the network having professional oversight, the availability of advice and users being bound by corporate-style policies. The user loses freedom of use (as they are in effect living at work) and gains support that includes enhanced layers of security. On the other hand, the case of private accommodation blocks providing this facility could be considered a worst-case scenario. For example, to reduce infrastructure costs, the network might be WiFi-only. This makes it impossible for users to add extra layers of security beyond their endpoints, which are connected to an entirely unsegregated and unmonitored network populated by security novices.

The networks are safeguarded only by the same type of terms and conditions offered in cafés and other public WiFi networks — terms which mainly offer protection to the network provider. They are often under-provisioned to reduce cost, making bandwidth availability the greatest issue observed by the user.

In the first infrastructure the user has a limited amount of control over their own security — some ownership and control of the SOHO router at the perimeter is retained by the ISP, so the user has to build an additional perimeter to protect their devices. In the second infrastructure (Figure 21(c)) the user is entirely reliant on the BYOD network owner for their home security, which, depending on the operator, may be advantageous or otherwise.

5.1.1.2 *Single person companies*

The UK Department of Business, Innovation and Skills Business Population Estimates for 2016 state that 76% of the 5.4 million businesses operating in the UK employ only the owner [28].

The first notable characteristic of single person companies is that most do not have dedicated offices. The participants working alone away from home (3 of 11 in the questionnaire) worked in industries where they might need a studio or a workshop (they had the choice between their home office and using a managed network in their shared workspaces). The significance of this is that it can be assumed that where there are no dedicated offices there is no in-house dedicated network infrastructure — the individuals work in the home networks described in the preceding subsection.

Using the questionnaire data (11 single person companies) to describe the technology single person companies described: all but one of these respondents have a company website, and all but one has a smartphone or tablet containing company data. All respondents have one computer containing company data, half have two. All of the respondents with company data in more than one computer have stated that they issue company computers or phones, so it can be assumed in many cases that the second computer is their personal machine. Half of the respondents with company data on

only one machine do not issue company computers or phones, so it can be assumed that all the company data is on the respondent's personal computer.

Half of the respondents say they use webmail, and a different set of four respondents said they use cloud services to store data or use applications. All but one of the respondents have backed up their files and keep them off-site in case of fire. Only three of the respondents carrying out backups are not using cloud services. If a person is working alone from home it may be more difficult to find a free and secure place to store company data off-site, so it's likely that backups are one of the things these companies use cloud data storage for.

Half have suppliers or customers who provide a link into their IT systems, or who they allow to link into theirs. None of the respondents are in the security or IT sector, and only one of these companies gets an IT expert to set up their computer. All except one allows their operating system to update automatically and has antivirus software on their computers.

Five of these companies have their own social media accounts and use social media as their only or main source of advertising. Half of our single person company questionnaire participants stated that they have suppliers or customers who provide a link into their IT systems, or who they allow to link into theirs.

The resulting example network diagram (which, despite the addition of data, did not evolve during the interviews or triangulation) can be seen in Figure 21(d). Comparing this infrastructure with the requirements of the UK Government-endorsed Cyber Essentials Scheme [111], these companies have begun to implement some *malware prevention* measures and are *managing patches* (often manually) for their operating systems as a minimum. These would all fall under the category of 'basic measures' from earlier in this section. We hypothesise that these users are unlikely to have sufficient knowledge to understand the relevance of access controls in a single person company, or to want to invest in boundary devices, but the highest hurdle they will face pertains to secure configurations. (The limitations placed on SSITUs by their suppliers is explored in more detail in Section 5.4.)

The similarities between single person companies run without an office and home users is evident, but those working in shared studios, workshops or innovation centres also showed similarities with home users — specifically, those using the BYOD networks described in Figure 21(c).

5.1.1.3 *Micro-companies*

The majority of micro-companies in our study (excluding the single person companies) had dedicated offices, although the least customer-facing industries (four in our questionnaire dataset — from the transport and software development sectors) were still able to avoid this expenditure.

There is an immediate difference in infrastructure moving from a home setting into dedicated offices, as both the ability to host services in-house and the roles of system users change. This brings the infrastructure described by this group of participants closer to that described in the scoping section of the Cyber Essentials Scheme documentation [111]. Two very different types of infrastructure emerged (examples illustrated in Figure 22), but in both cases the size of the company means that they will still

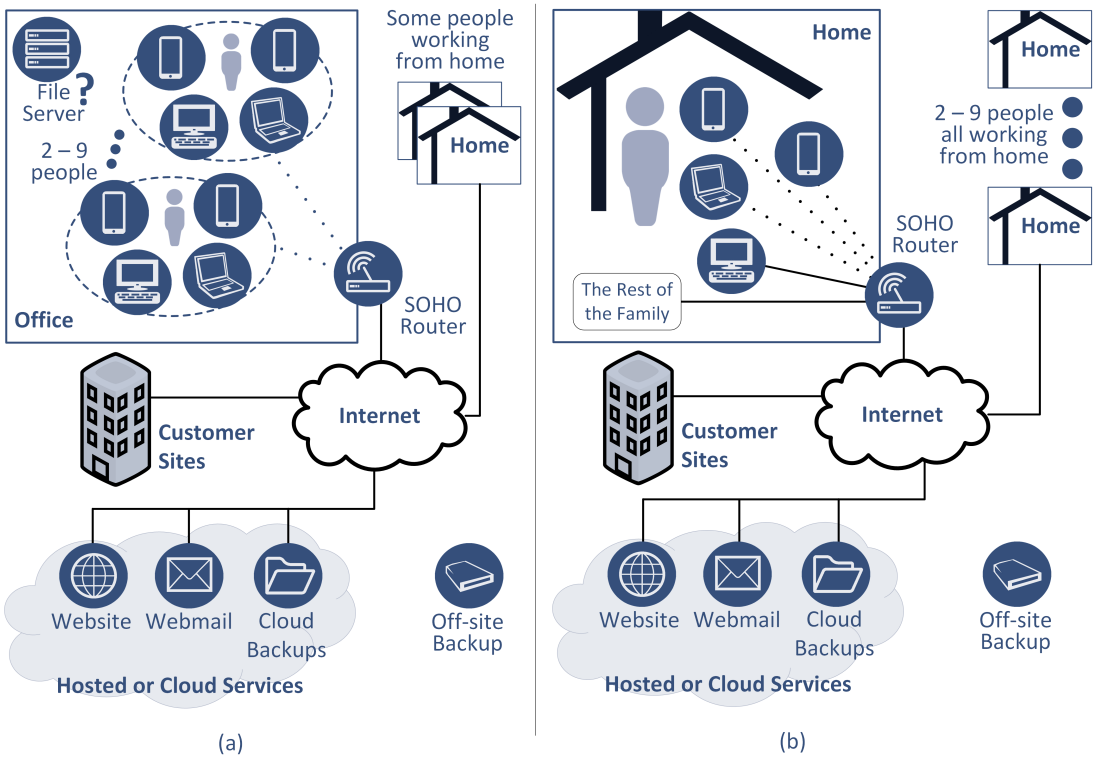


Figure 22: *Fragments of data analysis used to discuss results with participants: examples of micro-company infrastructure when using service providers' default settings*

be able to use (questionably secure[1] [40, 66]) small or home office (SOHO) routers. A third BYOD infrastructure was also present for companies of this size, similar to those discussed for home users and single person companies. This will be fully explored in Section 5.1.3.

Once again using questionnaire responses to provide data fragments: nine out of the thirteen micro companies who responded to this survey had dedicated offices; those without offices are working in industries which are not heavily customer facing, such as transport and software development. It is immediately obvious that there will be a difference in infrastructure when compared with single person companies, and two very different types of infrastructure, but the size of the company means that they will still be able to use small office or home (SOHO) routers.

These companies all have websites, and all have at least one or two smartphones or tablets plus one or two computers per person that hold customer data. Two companies indicated that people could have three or more computers, and tablets or phones per person. Most companies issue some staff with IT equipment, although three of the companies with dedicated offices do not. It is assumed that the increase in devices per person is due to a lack of a strict IT policy, rather than a higher requirement for multiple devices per person.

The increase in company size has not reduced the number of companies using webmail, and half the respondents still use cloud services, irrespective of whether or not they have dedicated offices. All these companies have off-site backups of their data.

1 Shodan boss finds 250,000 routers have common keys: `www.theregister.co.uk/2015/02/20/250000_routers_have_duplicate_ssh_keys/`

Three of the four without an office, and four of those with an office have suppliers or customers who provide a link into their IT systems, or who they allow to link into theirs.

Six of the thirteen have dedicated IT support staff to set up their computers, and another two identify themselves as being in the IT and telecoms sector themselves. All the companies let their operating systems auto-update, and have antivirus installed on their company issued machines.

Eight out of thirteen have their own social media account, but only two state it is their only or main source of advertising.

The use of cloud services and logical links with customers or suppliers remains prevalent in micro-companies, so the availability of an office in which to house servers, etc. does not have a great impact on the hardware choices made by micro-companies. In the first infrastructure (Figure 22(a)), where all employees are centralised in a single office, it will become more feasible to consider the first set of controls suggested by Cyber Essentials: *boundary firewalls and internet gateways* [111].

The biggest difference between the two infrastructures is the number of SOHO-routed networks encompassed when employees are distributed in their homes, as can be seen in Figure 22(b). This will have an impact on both the types of activities and the number of user roles existing within the scope of the corporate system. These are discussed in more detail in Section 5.1.3 and Section 5.3 respectively.

5.1.1.4 *Small and medium companies*

All of our participants working in companies consisting of between 10 and 249 people have dedicated offices. Companies where all staff are based in the same location are becoming too large to use SOHO routers — meaning that they are beginning to use elements of corporate IT network infrastructure. They all describe, as a minimum, applying the same basic cyber security measures as smaller organisations.

Comparing these businesses to those in the preceding two sections: all the companies have websites, all have at least one computer and all but two have at least one smartphone or tablet each. All these companies are issuing IT equipment to some of their staff. Interestingly the number of phones and tablets per person in a small company emulates that of a micro company, while both medium-sized companies state that people only have one of each. A larger dataset might show that this is the point where companies become large enough that they cannot avoid implementing and enforcing a strict IT policy.

Only two out of the twelve respondents are using webmail for work, one of whom has qualified their response by saying they're using a cloud service to host their own email server. Only three of the companies are not using cloud services. Only one company is not backing up their files.

Excluding some companies in the IT sector, companies of this size employ expert IT support, meaning that their infrastructures are often more corporate in appearance, allowing for the application of some more evolved security measures such as firewalls and monitoring systems; it also means that their security policies appear more mature. In medium-sized companies the average number of computers holding company data per employee reverts to one, in line with controls of large corporate entities.

Our study indicates that companies of this size have sufficient control of their networks and devices, as well as the expert support required to focus on the elements of

Cyber Essentials that smaller organisations typically struggle to achieve: *secure configuration* and *access control* [111]. Some of these organisations had sufficiently mature cyber security capabilities to be introducing some of the elements of the UK Government's *10 Steps to Cyber Security* [112] not included in Cyber Essentials: monitoring, incident response planning, and user education.

The smallest of these companies have limited differences in their infrastructure when compared with those of the micro-companies, as illustrated in Figure 22. To show how infrastructures might evolve from this point, Figure 23 (which is reproduced from our initial SME-focused technical report [70]) focuses on two participants from medium-sized companies, and their differences. Both of these companies have between 50 and 249 employees, but only one has implemented an architecture containing elements that may be more familiar to a large organisation. In this case the difference between the medium and the large organisations would be in the level of security specialism and redundancy in the IT team, as the system is still comparatively small, but these differences are sufficiently subjective to disqualify some medium-sized organisations from our SSITU stakeholder group.

The second medium-sized organisation has taken a strategically different approach, making their infrastructure appear more like two amalgamated micro-companies than one larger company — using this strategy a company could grow beyond 250 employees and still remain a SSITU, depending on the maturity of their security policies and the size of their IT function. This approach is discussed in detail in Section 5.1.3.

5.1.2 *Infrastructure by maturity*

Not all small organisations are startups: some organisations begin with the intention that they will remain providing relatively small services to a local community — one participant, for example, gave the example of a small drinks manufacturer.

Our study showed that these organisations often have IT systems that reflect the adaptation of their working practices over time to include technology. They are more likely to have fixed IT infrastructure (consisting of, for example, cabled networks, switches, and servers managed in-house (or by outsourced IT services, rather than cloud service providers)) than a similarly sized, but more recently established organisation.

In such organisations the use of local hardware, rather than cloud services means that, depending on the point in the hardware life-cycle, they may be under- or over-provisioned in terms of both digital storage and computing power. The inflexibility of using hardware in-house at this scale also increases the risk of limited redundancy should there be a need to recover after an attack [134].

Mature companies are more likely than a startup to have legacy processes and lack security awareness. Measures such as resilience are more likely to be implemented after an attack, once the organisation realises how much they have grown to rely on technology for business continuity.

The greatest security vulnerabilities in these types of organisation come from the organic introduction of technology over time. This lack of strategy when introducing technology into the organisation leads to an inconsistent infrastructure, potentially without clear ownership, and containing unsupported legacy equipment.

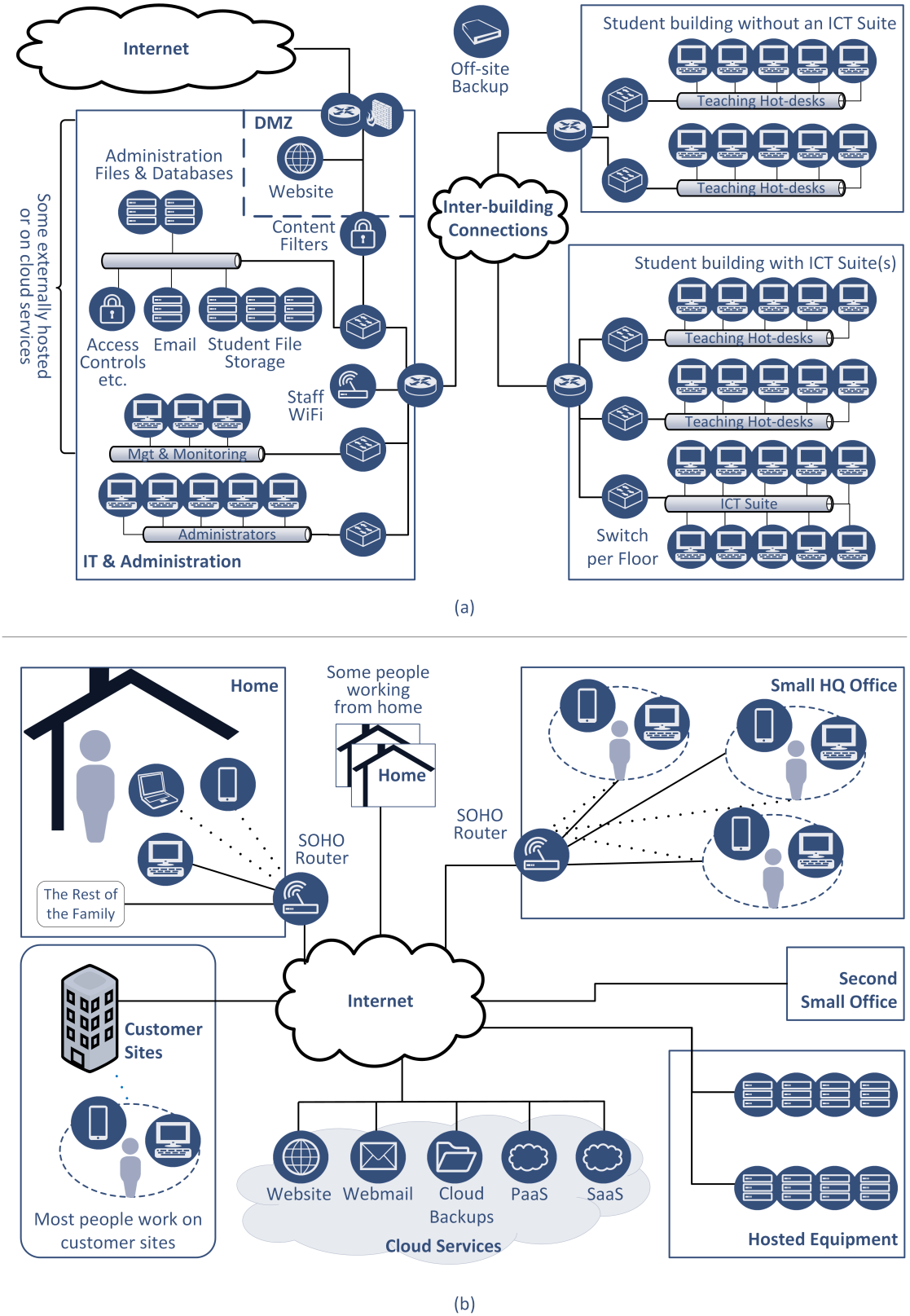


Figure 23: *Fragments of data analysis used to discuss results with participants: examples of medium-sized company infrastructure; (a) from a business subsequently excluded from the SSITU definition due to the scale of their technology use; (b) displaying an example of a larger, but still low infrastructure business*

5.1.3 *Infrastructure by strategy*

We now draw together a number of factors highlighted by our participants that may influence the strategy they develop for introducing technology into their organisations. These factors include industry sector and its influence on the number/size of the offices they maintain, the computer-literacy of their employees, their use of technology, and the level of investment this warrants. In the following, we describe strategies that avoid the adoption of larger corporate networks described in Sections 5.1.1.4 and 5.1.2.

5.1.3.1 *Low infrastructure organisations*

A number of elements in the infrastructure of organisations could make them what we term *low infrastructure organisations*. Our participants described 20 organisations, using varying degrees of low-infrastructure system. These are entities that have made a strategic decision to structure their technology use so that they require very little physical office space or company-owned infrastructure. One participant from the medium-sized enterprise illustrated in Figure 23(b) chose to describe their infrastructure thus:

> *"From the start we have taken an approach of not having much, if any, on-premises IT systems. As a consequence all of our business systems are either provided as software as a service (SaaS) (for example the HR system) or as platform as a service (PaaS) (using AWS). We also use co-location facilities to host some equipment. In addition most of our employees work at customer provided facilities and we have a single small HQ office with a number of us working out of our homes. We use Office 365 as our email solution."*

This is the type of infrastructure advocated by some cloud researchers [19], requiring extensive use of SaaS or PaaS to replace physical infrastructure and estates. SSITUs employ a wide range of cloud services. Despite this, there was a lack of discussion from participants about the value exchanged when using free services and the impact this might have on the value of their intellectual property.

Many SSITUs see the cloud paradigm as an ideal solution for improving security, as service providers should provide far better protection than the user can implement for themselves.

Participants made no mention of distinct cloud security measures, meaning that although they expect the cloud to be more secure they are not introducing new security measures of their own. SSITUs did highlight a lack of affordable cloud services who advertise themselves as having a security accreditation. (A secure cloud solution accredited by the UK Government was considered by our participants to be beyond the means of small organisations.)

The following is a list of common attributes described by our participants in implementing a low infrastructure strategy.

- The majority of employees work from home or customer sites.
- The broad use of cloud services to allow flexible growth.
- The dedicated offices used by these organisations are very small in comparison to the size of the organisation — in comparison with the mature organisations

discussed in Section 5.1.2 these organisations have very little hardware per employee.

- The small 'real world' presence these organisations have is mainly used to host high value assets (such as intellectual property) that the organisation does not want to entrust to another organisation.
- Growth doesn't imply transition to larger network infrastructure. If there is extra resource available for growth, it is used to build redundant offices rather than increase the size of the head office.
- Offices are kept small enough (8–10 people per office) to function behind SOHO routing.
- Limiting the size of the offices maintained allows low infrastructure organisations to use only consumer devices when selecting technology, with security mainly being policy-based.

The lowest infrastructure organisations are entirely virtual — examples of this in the dataset tend to be charities or private clubs. In these cases the organisation operates without any of their own investment in infrastructure beyond having a hosted website. All online activities are carried out via utilisation of the networks and equipment is paid for by the organisations' members, volunteers or employees. This is an extreme extension of the BYOD model, where the users have no choice but to provide the infrastructure themselves thereby reducing the costs of the organisation and limiting their perceived responsibility for good cyber security practices.

In the case of virtual organisations it becomes impossible to implement physical security measures, which, for example, $(ISC)^2$ suggest make up a key pillar of cyber security good practice [38] — the organisation only exists in cyberspace. That means that these types of organisation are far more reliant on other, logical or policy-based, cyber security measures.

This highlights another element of how infrastructure impact security models — as well as the age and size of an organisation impacting the systems organisations put into place, there is also the link between the size of the estate needed for the company to function and their infrastructure. startup companies can have a low infrastructure strategy; however, if their core business model requires them to have a large estate, it is less worthwhile trying to outsource all IT services to the cloud. The most obvious examples of this in our dataset are an educational establishment and innovation centres.

The former, one of our medium-sized enterprises, is illustrated in Figure 23(a) and is possibly the participant with the highest level of fixed infrastructure. The reason for this is that, unlike other industries, educational establishments usually have a requirement not only to provide IT services for their staff but also for their students. Our survey does not provide detailed information about the number or ages of the students; as such, we have given consideration to information provided by schools who list their ICT facilities on their website: one example school, which has 162 staff members and 1420 pupils (not untypical for a UK state school), has 8 ICT suites, each consisting of 32 PCs and an interactive whiteboard; further, each individual teacher's room has access

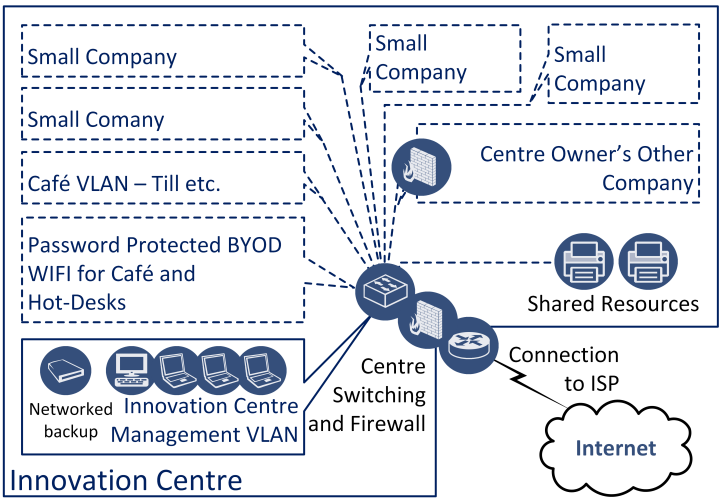


Figure 24: *Data fragment: an example of an innovation centre system architecture*

to a PC[2]. As discussed in Section 5.1.1.4, at this scale this type of organisation can't be considered a SSITU.

With respect to the latter, innovation centres are small organisations run by a handful of people that supply infrastructure to a number of other businesses. These businesses pay for infrastructure as part of the service, with a segregated, secure network being a key part of that provision. The innovation centre has inadvertently become a product-embedded SP, as described in Chapter 2, with significant influence over the quality of their clients' security. Figure 24 shows one of these networks as described by the relevant participant.

5.1.3.2 *Multi-purpose infrastructures*

As discussed in preceding sections, the infrastructure employed by many small organisations do not typically match models used by security experts in the development of advice and standards. The multi-purpose infrastructure model described here intersects with the low infrastructure model described in Section 5.1.3.1, BYOD models and the use of cloud-based computing. At least 14 of our participant organisations leveraged multi-purpose infrastructures.

By far the most important deviation from standard security good practice by our participants is in the multi-use nature of the networks employed by them. Cyber security good practice, as explored in Chapter 2, implies the segregation of activities within a network so that appropriate access control measures can be applied [38, 111, 5]. While there was evidence that SSITUs often not only fail to employ these elements of good practice, our participants were actively increasing the number of uses they made of the only infrastructure they were required to purchase — as the minimum level of resource they could procure was greater than that required for any single activity. Figure 25 shows an example from our dataset of a home network used by both a family and single person company.

2 www.mountbatten.hants.sch.uk/home

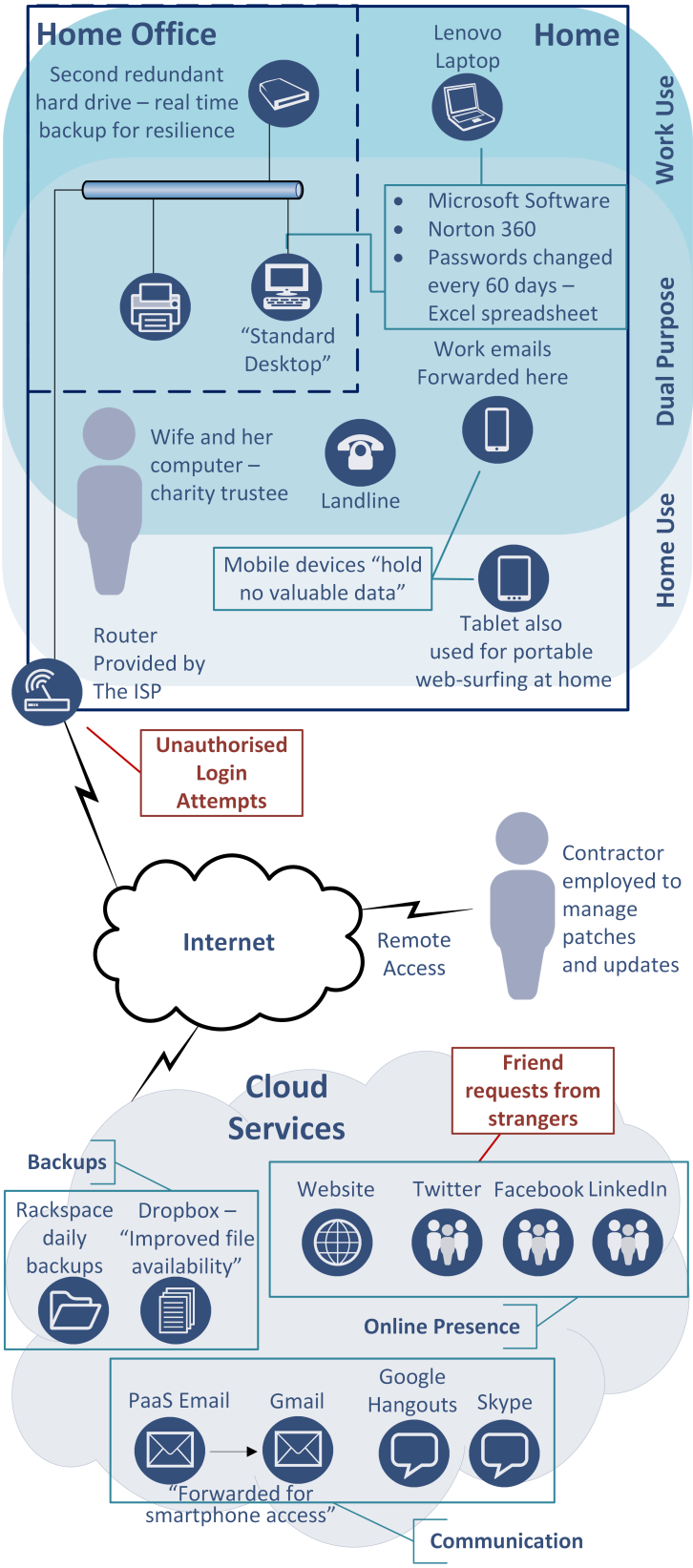


Figure 25: *Data fragment: an example of a multi-purpose home system architecture*

In our dataset, the segregation required in order to implement rigorous access control policies was limited in a number of ways:

- Clubs and charities may have no physical presence, so home users might be using their infrastructure in a volunteer role.
- Low infrastructure organisations may expect employees to use their home networks.
- Startups may expect to have IT infrastructure provided as part of the office space they rent.
- Small business owners may display limited work–life separation.
- Single person companies may share a network with a family.
- Most large companies will expect to have sufficient numbers of employees working from home that they are forced to include this in their IT policies.
- SSITUs often use personal devices for work.
- Individuals and small organisations may have little or no control over the network they rely upon for work.

The relationship between infrastructure use and process varies: in the large corporate model, differentiation is often at a network level; in small organisations, differentiation may be at a device or application level (or not at all).

Multi-purpose infrastructure exists in all sizes of organisation; however, as an organisation grows, it becomes more likely that there will be some separation of roles due to the provision of company-owned devices for this purpose. These company devices will connect with the company network via a VPN, reducing the device's interaction with outside systems.

With the concept of segregating systems and segregating roles being at the heart of cyber security good practice, the pervasive issue of small-scale IT users needing to use infrastructure for multiple purposes has a significant impact on security.

5.1.4 *Defining a perimeter for security?*

The IT support providers participating in this study all segregate their different customers for reasons of security; as such, those small organisations using a traditional IT outsourcing model are more likely to have a defined system perimeter. In contrast, as mentioned in Section 5.1.3.2, companies small enough to operate from an individual's home will typically have difficulty separating the different functions carried out within the network.

Many participants had a working assumption that the networks they used were insecure. One participant described how he considered mobile networks to be more secure than free Wi-Fi he could obtain in the same location, but he generally preferred to use his laptop in the home network to complete what he defined as higher risk activities — anything involving a financial transaction, for example. Some participants described attempting to protect assets such as credentials by not storing them on devices they expected to be insecure.

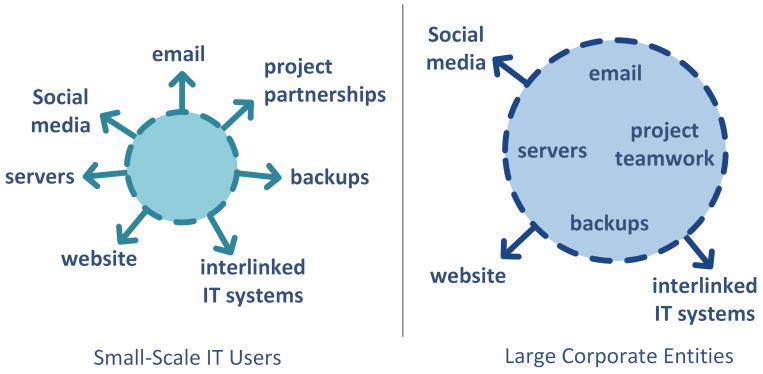


Figure 26: *Analysis fragment: abstract network diagram from an SME case study*

Another issue highlighted for small organisations is mapping infrastructure and digital assets. Although this is complexity that is often thought to be associated with size, the lack of formal policies about which online services are suitable for an organisation — plus the use of personal devices — also makes it an issue for small organisations. In some cases it may be impossible to map an organisation's digital assets, not least because they may be using cloud services unwittingly.

The broad use of cloud services for backups, data sharing and collaboration is evident. This may be a result of formal policy or a consequence of need. As shown in Figure 26, this produces an organisation with a very limited core infrastructure when compared with a large organisation, with the use of large numbers of third-party services producing a proportionately far greater perimeter to secure. This means that, as a result of system architecture, the attack surface for a small organisation may be greater than that of a large organisation.

Pfleeger and Pfleeger suggest that an element of cyber security good practice involves managing investment in security measures to protect the most valuable assets [80]. This works for large organisations where large-scale security mechanisms are cost-effective and there is sufficient infrastructure to build multiple layers of measures around their critical assets.

In describing the security decisions they made, SSITUs placed emphasis on pragmatic decisions and employing only adequate security. Small organisations struggle to reach the critical mass where it is cost-effective to employ anything more than endpoint security. Their most valuable assets hold a proportionately higher value than the assets owned by large organisations, but it does not necessarily follow that they have the ability to protect themselves more effectively. The infrastructure described in this section are not best adapted to the defence-in-depth model described by [25], because they are unable to facilitate Carroll's principle to *"concentrate your valuable assets so they can be protected"* [21]. This means that for valuable items such as intellectual property small business owners are still relying on obscurity to keep their assets safe.

SP stakeholders highlighted the issue of unexpectedly poor policies in small organisations. This lack of engagement with 'free' aspects of implementing cyber security are thought to indicate SSITUs' lack of knowledge. As one participant stated, "security measures don't make decisions, people do"; however, the majority of SMEs in our study favoured technical solutions that could be installed and ignored. None of the

SSITUs described any provision of a reactive security budget for mitigating against unknown unknowns.

Business-owning participants made decisions that favoured availability over confidentiality and favoured resilience over security. In contrast home users limit, or partition, their choice of services to retain control of privacy and security.

5.2 IMPLICATIONS OF EMERGING CONSUMER CYBER PHYSICAL SYSTEMS

In Section 5.1 we explored the existing systems described by our participants, but the technology used by consumers evolves rapidly, making it worthwhile to explore an emerging type of system — *Consumer Cyber Physical Systems* (Consumer CPS) — that has the potential to influence the security of the IT systems used by SSITUs.

For the sake of clarity, Consumer CPS are considered to be consumer products containing embedded systems that take advantage of the increase in available wireless technologies to connect to the Internet.

As highlighted in Chapter 2 a close relationship has existed in the fields of cyber security and safety for an extended period. In this section we focus on the emerging context of ubiquitous computing and pervasive connectivity — in which safety can often only be maintained through cyber security. In particular, we argue that the traditional views of 'safety' and 'security' will, inevitably, have to adapt to this new reality.

It is worth highlighting at this point that our datasets showed a divergence of opinions where the intersection of safety and security are concerned. As mentioned in Chapter 2 safety and consumer rights are strongly embedded in the expectations of end users, so even with the occasional SSITU participant mentioning that they are beginning to adopt networked home appliances, it was mainly the RH stakeholder group describing cyber-physical risks in the home.

One example was a safety expert concerned that the development of Internet of Things devices should be focussed on *augmenting the performance* of consumer technologies, but as highlighted in Chapter 1 adaptation of devices for the Internet of Things is often a marketing-driven exercise. In another example, a security expert at a large critical national infrastructure organisation described the risks associated with SSITUs joining both their physical and IT infrastructures as extremely small but numerous stakeholders.

In an extended version of this section ([72]), we compensated for a lack of data about these emerging systems with the use of scenarios[3] based upon the types of Consumer CPS already available, taken from different business sectors, e.g. Proofpoint's spamming fridge[4] and smart climate control systems as reviewed by CNet.[5]

5.2.1 *The emerging context*

Table 9 identifies a number of service sectors where ubiquitous computing may have an impact, together with the locations where a consumer might come into contact with

3 A full description of the scenarios we use can be found in Appendix B.

4 http://www.proofpoint.com/threatinsight/posts/your-refrigerator-is-full-of-spam-part-ll-details.php

5 http://www.cnet.com/uk/news/smart-home-climate-control/

Sector	H	W	T	R	S
Buildings	•	•		•	•
Energy & Water	•	•		•	•
Consumer & Home	•	•		•	•
Healthcare & Life Sciences	•	•	•	•	•
Industrial & Agricultural					
Transportation			•		
Retail			•	•	•
Security & Public Safety			•	•	•
IT & Networks	•	•	•	•	•

Table 9: *Consumer contact with IoT sectors*

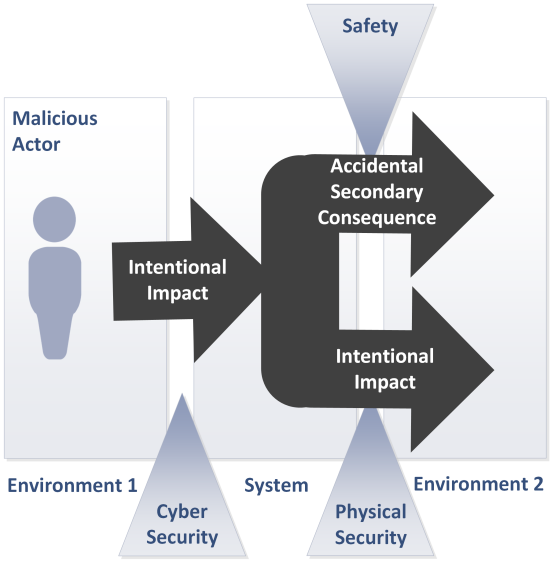


Figure 27: *Use of the definitions of* safety *and* security

them in a 'typical' day: home (H), work (W), transport systems (T), retail outlets (R), and social spaces, such as restaurants and bars (S).

The table demonstrates that the only commonly defined sector for ubiquitous computing that a consumer does not come into direct contact with is the industrial and agricultural sector. Somewhat ironically, this sector, along with the non-public-facing aspects of energy and water production, are those most commonly discussed when considering the synergy between safety and security [82, 94, 29].

As computing becomes ubiquitous, the lines between IoT sectors are likely to blur as new services themselves provide new opportunities for services.

In the background chapter we explored the definitions and convergence of security and safety models. In this section we base our definitions on the *SEMA* referential framework of [83], introduced in Chapter 2. To this end, we characterise safety and security risks thus:

- *Safety* risks originate from the system, accidentally impacting on the environment.

- *Security* risks originate from malicious actors in the environment, intentionally impacting the system.

We characterise the *environment* of these definitions as "the set of other interacting systems whose behaviour and characteristics are generally less known and beyond the control of the system owner" [83]. For the purposes of this section, this definition is assumed to include the physical environment and underlying communications systems, although Consumer CPS are assumed to be complex systems in their own right.

Figure 27 shows how these definitions are interpreted in the context of interest. The risks discussed encompass aspects of both safety and security, examining use cases where it is possible for the actions of malicious parties to impact on the physical security or safety of the environment. Environments 1 and 2 could be the same environment, or entirely different environments due to the increased interconnectivity of systems inherent in ubiquitous computing. Consumer CPS are thus differentiated from typical consumer devices by their capacity to cause physical harm in the local environment (Environment 2) following networked intervention from Environment 1. Most strikingly, Figure 27 shows how internet-connected devices could pose a safety risk to the inhabitants of Environment 2.

Cyber physical systems combine the physical (continuous) world with the digital (discrete) one [85]. Until now, development of distributed CPS has mainly occurred within safety-critical systems; however, consumer devices in the Internet of Things can be considered as a type of highly distributed CPS.

Wolf et al. [125] discuss the fact that constraints present in traditional CPS for real-time communication and safety are less present in consumer systems. They argue that this opens the market for the widespread sale of data, actuator or computation services, in line with the IT-driven business models [46] described in Chapter 2. The inference is that, in being less bound by safety regulation, Consumer CPS designers can produce the innovative products that would lead to ubiquitous computing far more rapidly than safety-critical systems have been adopted in the past.

The number of products such as household appliances with embedded systems that could potentially go on-line are far more numerous than non-embedded systems currently are [93], implying a high-impact security issue. Despite this, as well as the expectation of designers to have fewer constraints, consumers have a preconceived idea of the acceptable price of an appliance, making the budget to create solutions extremely small [93].

Much of the research undertaken on CPS that reach the home has been in the context of *Smart Grids* [94, 85, 47, 63]. In such a scenario, the security focus is on protecting electricity company assets in a hostile environment — the consumer's home. Our focus throughout this dissertation, on the other hand, is consumer safety and security, and, consequently, any existing models where service-provider security is the focus may need to be adapted accordingly.

As summarised in Chapter 2, there are a variety of pieces of legislation at both UK and EU level designed to protect consumers. The complexity of both programmable systems and the legislation make it difficult to define how cyber security is included in consumer rights such as services provided with "reasonable care and skill" [113]. In general, as described in Figure 6, where safety measures have not been standardised manufacturers are expected to revert to *safety engineering* best practices — where possible making something intrinsically safe, and if not then defining a threshold of

tolerable risk [97]. In the context described in Figure 27, this would signify that safety engineers need to evolve to consider software a dynamic element of the system and add cyber security evaluations to through-life product safety considerations.

The IT-driven business models discussed in Chapter 2 highlight how the evolution in technology is changing the complexity of the systems consumers interact with. The modularity introduced by these businesses makes it far more difficult to judge the risks associated with the use of the system once it is connected. This is a particular concern for our risk-holding participants who described how increased numbers of small stakeholders increases the complexity and the source of vulnerabilities for the larger stakeholder.

Product designers now have to consider the integrity of the new services they are offering and the cyber security of the platforms on which they are hosted. As illustrated by Figure 27, by connecting a Consumer CPS to the Internet, new risks are introduced in the safety and physical security domains. While the new business model reduces the cognitive workload of the consumer, the broadening scope and complexity of safety and security requirements could over-burden system designers. We argue that developments in safety and security modelling techniques and frameworks should aim to address this issue in order to be adopted in the future.

5.2.2 *New sources of risk*

With the implementation of new services in the Consumer CPS market, the types of risks associated with products are evolving to include new hazards. We highlight some of these in the following.

5.2.2.1 *Remote operation of devices*

As highlighted by the scenarios one of the reasons for providing add-on services is to allow 24/7 connectivity to devices and the possibility for remote operation. Of course, operating devices remotely introduces new types of risk due to the operator not being able to assess the state of the environment as part of the decision-making process. One participant went as far as to suggest that they would have no control over the remote updates carried out by Internet of Things devices, so remote operation may be carried out by more than one entity.

Operators will not know if there are other people dangerously close to an appliance, or carrying out maintenance, or even if there are now objects in the way which may be damaged by their actions. In the climate-control example, turning on specific types of electric heater if there are items of clothing draped over them could be enough to start a fire.

The operator's lack of presence may also affect the magnitude of an incident; for example, if a malfunction leads to a fire the fact that there is no one present in the building may mean that it takes far longer for the fire to be detected and put out.

Another implication of the remote operation of appliances is that those operations will be changing the internal state of the device at a distance. Should the network connection be severed part-way through an operation, or before a critical update, the device could be left unsupervised in an unsafe state.

5.2.2.2 *Data integrity*

Non-networked appliances are unlikely to be programmed with cyber security in mind — it is unlikely that signals will be tested for authenticity as those signals will probably originate from a component fixed to the same circuit board; in the case of safety-critical functions, there may be limited tests for accuracy. Once an appliance goes on-line, with control signals coming from mobile phone applications or via a web-site, the designer can no longer consider the appliance as a closed system. If the appliance doesn't have a closed system, the integrity of data received by the controller might be compromised more easily. It might be very easy for a neighbour to use the link a refrigerator has with its owner's supermarket account to submit an order for their own food, or for the climate-control system to pass incorrect information to the fire-alarm system. The latter could result in an obvious safety issue; however, both of these examples could also cause financial losses for the consumer, leading back to the question of how cyber crime is handled, as per Section 5.2.1.

5.2.2.3 *A third party's motivation to use resources*

Proofpoint's incident report of January 2014[6] was related to the use of various devices as resources to use to send spam. The motivation of third parties to enumerate devices and transform them into resources introduces an entirely new type of risk to the household appliance sector — a direct consequence of increased interconnectivity. Of course, one may take the position that a refrigerator that sends spam is more entertainment than hazard, but, if instead of the refrigerator scenario, we consider an in-car media example, the consequences of an attacker borrowing computational power from one of the car's in-built controllers could be quite serious.

Data exchanged by the networked devices may also be used as a resource, damaging the privacy and potentially the physical security of consumers. Eavesdropping on conversations between a refrigerator and its owner's dieting and supermarket applications would give an attacker information about what they ate, but also highlight some health issues and bad habits that they might not want others to know about. If a climate-control application and an in-car media application are both linked in to the car's satellite navigation system they could provide an attacker with with owner's physical location — either putting them in danger or proving to a burglar that they are not on their way home. This ties to the privacy and confidentiality issues discussed in Chapter 2.

5.2.2.4 *Malfunction*

The increased complexity of the system, coupled with the potential number of stakeholders, makes it a challenging task to identify all of the potential flaws associated with a Consumer CPS, particularly should an element of the system reach end-of-life and cease to be supported. Malfunctions caused by cyber attacks, as outlined in Section 5.2.1, are even more concerning as the 'accidental' safety implications of an attack can be replicated either in multiple appliances or multiple times by persistent activity on the same appliance. If ongoing system verification becomes harder to achieve, there is

6 http://www.proofpoint.com/threatinsight/posts/your-refrigerator-is-full-of-spam-part-ll-details.php

increased risk of malfunction leading to injury, damage of possessions or the product self-destructing. UK fire statistics show that malfunctioning electrical appliances are a fairly common cause of fires within the home.[7] It may be the case that the increase of risk of malfunction in a Consumer CPS due to faults (or even malicious actors) might have the potential to increase the risk of fire within the home.

5.2.3 *Cyber security requirements for maintaining consumer safety*

A pragmatic approach is needed in order to encourage cyber security measures in Consumer CPS – that manufacturers would need a clear financial motivation which the connection between cyber threat, health and safety and product liability the system attributes described in Section 5.3.2 provide. In the context of a consumer cyber-physical system it is possible to use the definition of safety supplied in Chapter 2 as the catalyst for the first requirement:

A. Unskilled users can safely use the system through any recognised interface. *(system attributes 1, 3,16 and 17 also support this requirement)*

Using the thought processes applied by Pièvre-Cambacédès and Chaudet in the SEMA referential framework [83], it is possible to consider this requirement in the context of the sub-notions of safety and security it covers (Figure 28). As demonstrated the requirement is linked to three notions related to safety, but not to security. The addition of the other legal obligations discussed in Chapter 2 – Data Protection and Consumer Rights – increases the coverage so that all six notions are partially addressed, however there is a visible lack of coverage of the two main security notions, visually describing the lack of consideration of cyber security in the implementation of safety measures in Consumer CPS.

As we have argued throughout this chapter, the inclusion of cyber security is key in maintaining safety once the marketplace adapts to the pervasive availability of connectivity discussed in Section 5.2.1. In order to address these security concerns, we have selected a holistic framework for traditional information security, whose definition covers the three 'malicious' notions of the SEMA Referential framework. This framework makes no mention of safety, but provides a comprehensive set of "system-level security principles to be considered in the design, development and operation of an information system" [83].

The following four requirements, based on the system attributes fully detailed in [72], are aimed at bridging the gap between engineering practices when considering safety in information systems or cyber security in consumer products, in order to facilitate requirement A:

Design & Implementation:

B. Cyber threats are recognised as a potential safety hazard in networked consumer cyber physical systems, in order to maintain tolerable risk thresholds. *(prompted by attributes 2, 7, 21, 22)*

7 https://www.gov.uk/government/collections/fire-statistics-great-britain

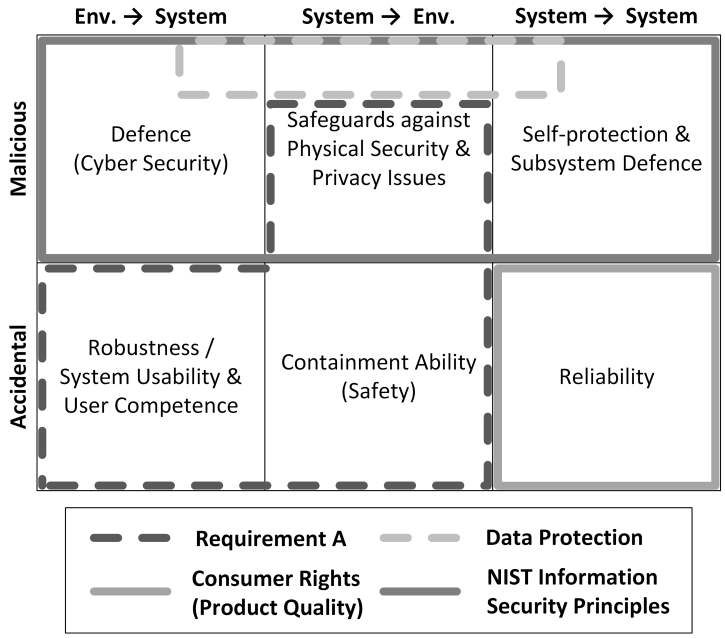


Figure 28: *Use of the SEMA referential framework in the context of Consumer CPS*

c. New sources of harm introduced by the network or connected subsystems (including, for example, harm to economic well-being and privacy only typically addressed by security measures) are evaluated. *(prompted by attributes 4, 5, 8, 24, 25)*

Through-life:

d. Modular designs are accepted in safety conformity accreditation so that products are considered as part of a dynamic system including add-on products or services, rather than as an isolated appliance or as a pre-defined system. *(prompted by attributes 6, 9, 11, 12, 13, 14, 15, 18, 19)*

e. Security degradation over time is minimised to maintain safety. *(prompted by attributes 10, 20, 23)*

For the new business models discussed in Chapter 2 to satisfy the original sentiment of safety legislation and reduce producers' liability, cyber security issues will need to be considered as part of the product lifecycle. While this is needed to maintain a level of safety equivalent to that currently experienced, there is a lack of clear legislation in this area, due to the complexity of aspects of the new business model being perceived as service provision rather than a product.

In Section 5.1 we described the infrastructure described by our participants, an overview that this section has enriched with the context of emerging cyber-physical systems. Figure 29 illustrates how the scope within which SSITUs can mitigate security risks is limited by the system infrastructure they employ.

5.3 Interactions and the digital footprint

As we saw in Sections 5.1 and 5.2, SSITUs have an increasingly complex online presence, with a significant portion of their systems existing in public cloud services. Risk

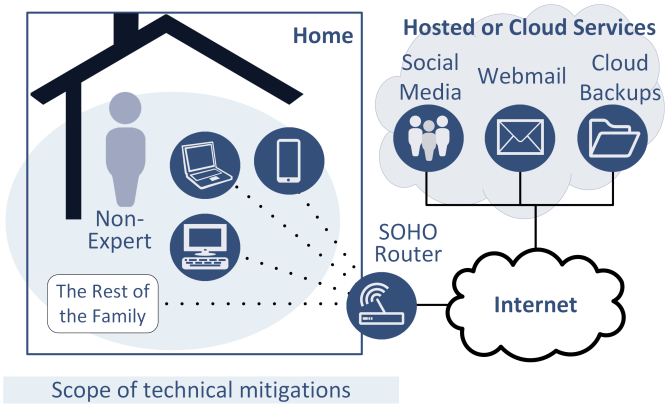


Figure 29: *Overview used to triangulate findings: the available scope of cyber security mitigation considering only user-controlled technical system elements*

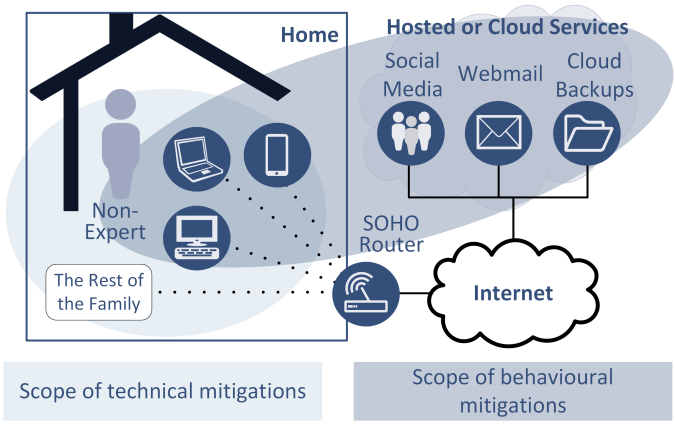


Figure 30: *Overview used to triangulate findings: the available scope of cyber security mitigation when including behavioural mitigations within the digital footprint*

assessment processes such as that described by [13] encourage larger organisations to include intangible risks in a typical cyber security scope, but investment in risk reduction tends to focus on technical security measures within a large high-infrastructure system.

The data collected in our study highlights how SSITUs need to consider how their risk extends to include their *reputation* (the most motivational of all the assets our SSITUs wanted to secure). For participants working towards a low-infrastructure system, reducing intangible risk requires mitigating within the virtual element of the system. In Figure 30 we illustrate how, by including the digital footprint, SSITUs are able to increase the scope of available security mitigations across their system beyond that described in Section 5.1.

To this end, alongside the infrastructure (Section 5.1) and system interactions (Section 5.4) that make up a typical cyber security discussion, we have included a SSITU's digital footprint — the scope of their virtual presence — as a vital element of the cyber decision-making process.

In this section we explore the definition and scope of digital footprints, their relationship with cyber security, and, finally, the implications of the interactions between

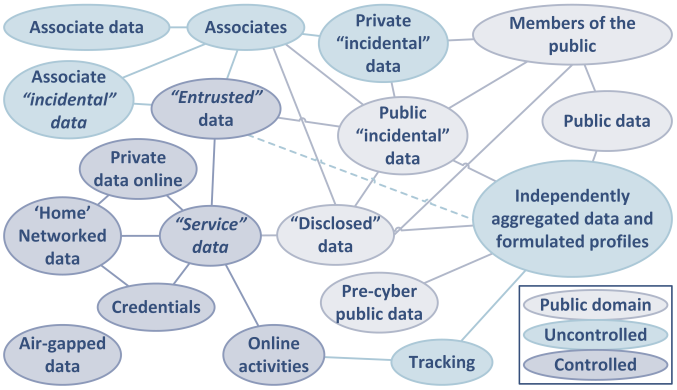


Figure 31: *Analysis fragment: digital footprint for a single user role*

different roles and third party decisions on elements of cyber security good practice, such as access control.

5.3.1 *The definition of digital footprints*

The Oxford English Dictionary definition of cyberspace discusses a *"notional environment"* where electronic communications occur, in effect creating a *"global village or sphere of human interaction"* [77].

Internet users, whether individuals or organisations, have to interact with a variety of technologies in order to access the network and interact with other users or machines. The scope of the cyber security function within an organisation typically concerns their IT system, alongside an analysis of the risks associated with allowing its use within certain parameters. Therefore, a company's definition of the scope of cyber security encompasses communications networks, data storage, human computer interaction, etc. — that is to say, all of the tangible (and so potentially controllable) interfaces with cyberspace.

Figure 31 shows some of the elements that may be considered part of a digital footprint for a specific role a user plays and its links to the wider community in cyberspace, via both a user's associates and their public disclosures. Here, we have used terminology from Schneier's *Taxonomy of Social Networking Data* [91] to clarify the content of some elements of the footprint. This concept of community makes a digital footprint greater than the sum of its parts [123], positioning it within an environment in which a SSITU's reputation can develop.

Cyber security good practice encompasses system elements that can be controlled to produce security — scope in risk assessments generally excludes uncontrolled elements of the system. However, emphasised within our dataset is the notion that small organisations wish to secure their reputation. Figure 31 illustrates the extent to which, at the interface with cyberspace, user contributions and the reactions from both associates and members of the public might shape a reputation.

Reputation is everything and community (and so increasingly the "global village" [77] of cyberspace) is the source of reputation. The *digital footprint* can be used to define how the scope of cyber security extends into cyberspace, by describing a SSITU's virtual presence.

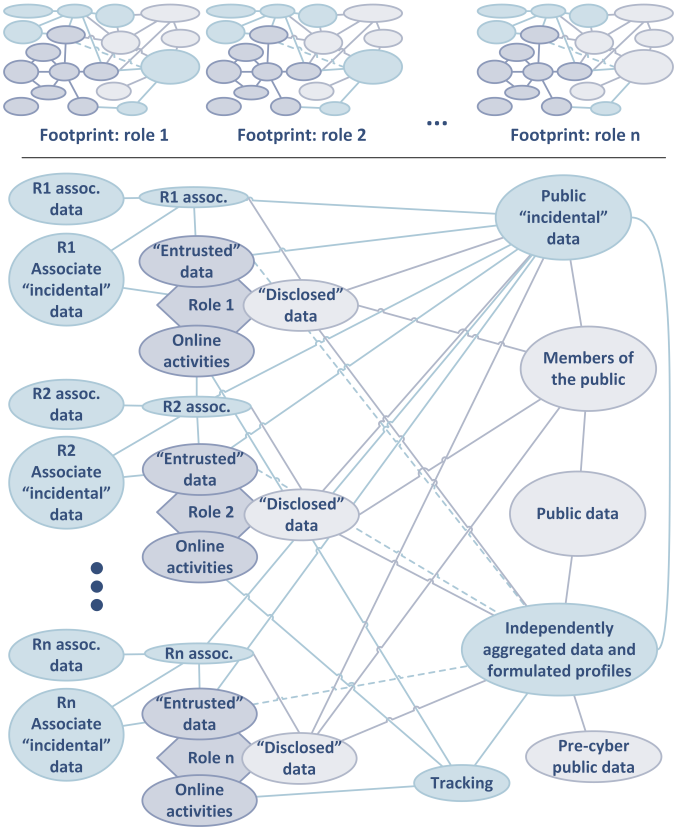


Figure 32: *Analysis fragment: digital footprint showing combined roles for a SSITU*

Weaver and Gahegan describe how a digital footprint can be made up both of a user's online activities and the digital artefacts produced by those activities [122]. In the case of SSITUs this could, for example, be the tracked browsing history of an individual, or the social media identity of a small company.

A digital footprint in our study can contain both user-created and user-moderated (*active* [58]) content and unmoderated/uncontrolled (*passive* [58]) content, related or attributed to the user. In Figure 31 there is even a category of data (private contributions to data in online services) that a user would have no visibility of — representing, for example, private conversations third parties might have about comments a user has posted.

A user's footprint is the sum of the virtual presence created for each role they hold. As Figure 32 shows, beginning to merge the footprints immediately introduces complexity into a user's understanding of who has visibility of which data.

Drawing upon an example from our study, one participant had a single person IT company, designing and hosting around 60 websites. He volunteers for a number of small charities and private clubs, and also uses the network for personal communication, web surfing, etc. Each of these activities contributes in some way to the participant's digital footprint, with the fact he constitutes a single person company increasing its scope and making it hard to differentiate the individual's footprint from that of the company. An illustration of this participant's digital footprint can be seen in Figure 33(a).

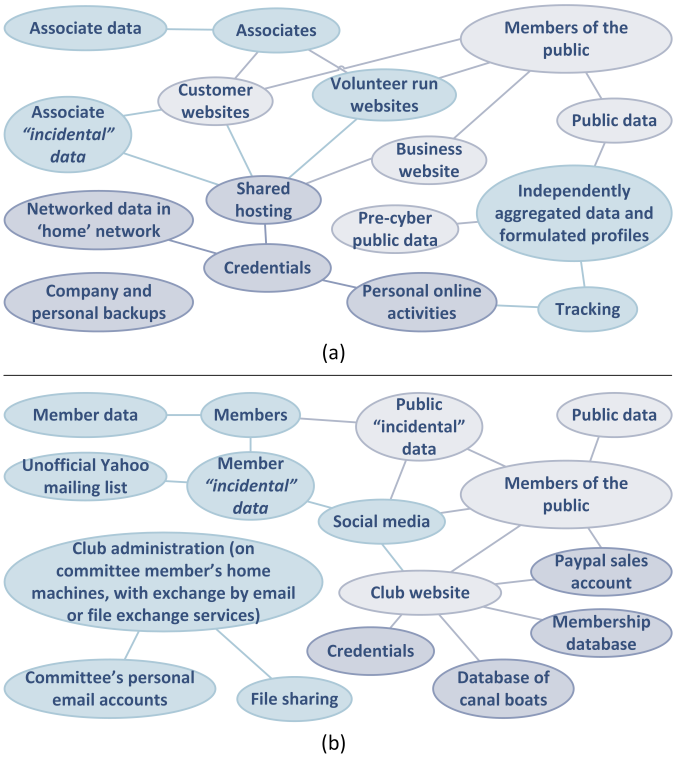


Figure 33: *Example of an individual's and an organisation's digital footprints from a participant in our study*

As discussed in Section 5.1, some organisations exist only in cyberspace. In the case study of the previous paragraph, the participant describes the digital footprint of one of the clubs he supports, illustrated in Figure 33(b). In their case, the website is the principal manifestation of their existence — a logical entity, hosted by the participant on servers owned by his company, with many of the club's other data held informally by committee members. Members have a variety of means for communicating with each other, either publicly or privately. The club has a responsibility, equivalent to that of a business, to protect its members' data, including their identity. However, unlike a typical business, the club is a virtual organisation. There are some organised events where members can meet in person, but the majority of the organisation's presence and its community's interactions are virtual. The club has no dedicated infrastructure, offices or trading address. For the most part, it exists only in cyberspace.

5.3.2 *Securing the virtual*

Oxford English Dictionary has a broad range of definitions for *security*, with one directly relating to information security:

> "Freedom from danger or threat —
>
> e. With reference to encryption, or telecommunications or computer systems: the state of being protected from unauthorized access; freedom from the risk of being intercepted, decoded, tapped, etc." [77]

SSITUs in our participant group making security decisions are reacting to a perceived risk — they are attempting to protect assets that have value to others, although the extent to which they protect them is based, as advocated in [80], on the value they have to the user.

As previously discussed, good practice applications of security measures tend to focus on the tangible elements of the system. This approach proves challenging in the context of entirely virtual SSITUs when they have identifiable security risks (in our example, the reputational risk of not protecting member data).

We suggest that, for SSITUs who lack the resources to opt for capital expenditure on their own infrastructure over the use of cloud services, having a digital footprint in cyberspace has as much relevance to security as any tangible element of the system. The composition of a user's digital footprint becomes critical to cyber security at the point at which it either introduces new risk or heightens an existing risk.

As well as reputational damage, other risks mentioned by our participants were:

1. the reaction to disclosures;
2. the scope and speed of diffusion; and
3. a heightened risk of social engineering.

Risk 1 was highlighted for different reasons. There is always a risk that a comment made will be misconstrued by someone in the audience, bringing attention for the wrong reason. Internet users also demonstrate a surprising inability to judge what information is credible before sharing it, for example mourning celebrities more than once[8]. Once something is immortalised digitally, it is often given more credibility or emphasis than it would otherwise have been. This risk was specifically highlighted as an issue where law enforcement is concerned — digital proof of an offhand comment suddenly gets investigated, even if it is just a joke in poor taste[9].

Risk 2 — the scope and speed of diffusion of information shared — could compound risk 1, providing information to unexpected audiences in addition to the target audience. This may stand alone as a risk when considering small businesses who share their product development processes as interesting advertising content, as in the example provided by [11]. This is an excellent way to retain customer interest and the connection they feel to the organisation, but creative processes and know-how might also be assets that the company doesn't want to fall into the hands of a competitor.

The third risk — social engineering — is also a problem for SSITUs: the majority of successful attacks described by participants involve mistakes made by a user. One participant highlighted how phishing emails are made believable by impersonating an organisation — also a major issue, as the impersonated organisation has no way of preemptively protecting themselves against attackers copying logos and other elements of their websites.

Social engineering is potentially an even greater issue where small businesses are concerned. Suppliers were treating them in the same way as individual consumers with respect to the implementation of security. However, a law enforcement participant highlighted that businesses tend to get targeted more than individuals because their

8 www.bbc.co.uk/news/blogs-trending-35363394

9 www.independent.co.uk/news/uk/home-news/twitter-joke-led-to-terror-act-arrest-and-airport-life-ban-1870913.html

bank accounts have more funds available. This, combined with the scope of the digital footprint published by the directors of the smallest organisations, may make them the most vulnerable class of SSITU in this respect.

Unlike the physical or more technical elements of the system, limiting or controlling a digital footprint can't be enforced by altering the infrastructure: for example, [58] highlights how a certain amount of the digital footprint is out of the control of the subject. The controllable elements relate to activities carried out online, so, in order to control the moderated element of a digital footprint, an organisation will have to limit its activities and those of its associates.

The club illustrated in Figure 33(b) has chosen not to include a forum on their website. Instead, they have an unofficial mailing list on Yahoo, administered by members and ex-members. The reason for this is to avoid the club's responsibility for the content shared on those sites and limit the reputational damage inconsiderate users could cause.

This was also explicitly stated by one of the participants in our initial study — who mentioned modifying their behaviour by "not visiting dodgy websites" as a means to reduce risk. This approach comes at a personal cost — the respondent in question was in a single person company without dedicated offices. This means that, in order to maintain cyber security at work, the respondent would also have had to modify online activities in their private life.

SSITUs in our study repeatedly stressed the importance of reputation on their cyber security decisions. In effect, what the participants in our study are trying to protect is something that is intangible — a goodwill on which it is hard to put a financial value. The lack of control of the digital footprint could limit a SSITU's freedom to use the Internet, so their expectation as consumers is that security measures protect their digital footprint for financial stability, well-being and the ability to learn and move on from mistakes within the online community.

This is mirrored by the findings of authors such as Von Solms and van Niekerk [121], who feel that the move from information security to cyber security fundamentally changes the scope with which we consider security and responsibility. Suppliers may have an increasing duty to protect their customers' freedom to use the Internet [121].

End users are increasing the scope of the cyber security definition to include additional elements of the definition of *security* that move the definition away from their computer systems and towards a more socio-technical definition:

> "The state or condition of being or feeling secure —
>
> a. Freedom from care, anxiety or apprehension; absence of worry or anxiety; confidence in one's safety or well-being." [77]

and:

> "Freedom from danger or threat —
>
> c. The condition or fact of being secure or unthreatened in a particular situation; freedom from material or financial want; stability, assurance (of rights, position, employment, etc.)." [77]

One law enforcement participant highlighted how suppliers such as financial institutions are encouraging this perception of security as their business model requires the high volumes of transactions only achievable with consumer confidence.

The following subsections discuss the impact of a digital footprint on SSITUs' security, as well as reasons why small organisations and their directors may be more susceptible to the risks posed from an extensive digital footprint than the typical employee of a large organisation.

5.3.2.1 *Vulnerable users*

The existence of uncontrollable content further differentiates security issues associated with a digital footprint from those associated with physical systems and software choices. Madden et. al. suggest that even users who do not use the Internet will still have a digital footprint, which, although not visible to them, may influence the people or organisations they interact with [58]; it may also heighten their vulnerability to certain crimes.

A regional law enforcement officer suggested during one of our interviews that identifying the most vulnerable users is difficult: the ability to protect vulnerable users in the local community is limited by a lack of information about threats to this (or any) group. In an attempt to identify vulnerable members of the community, the participant described how methods used to identify properties actively targeted for burglaries are being adapted to gauge the amount of advice and support needed by victims of cyber attacks, based on the number of times they have been targeted. This attempts to ensure that vulnerable users who only sustain small losses still get help. The participant outlined how the reaction by law enforcement to a cyber attack (and the investigating team) is usually dependent on the sum lost — all reported cyber crime is recorded, but only crimes of a certain magnitude are investigated and/or referred to the National Crime Agency.

Figure 32 simplifies the unification of digital footprints, inferring that the user has visibility of the whole footprint, strangers only have visibility of the public data, and an associate in a particular role has visibility of both data associated to that role and public data. The reality is that the user won't have visibility of the whole footprint, because members of the community have the freedom to privately create elements of the footprint and, as [122] suggests, it is difficult (even as the data subject) to completely map a digital footprint.

Vulnerable users are those for whom unmoderated content in their digital footprints may be harmful. These users are inherently vulnerable and fall into two groups. First, members of the community already considered vulnerable, due to age, disability or mental health, could also be considered vulnerable SSITUs. As IT users, these individuals could be less able to handle unmoderated content produced by trolls, or more susceptible to grooming [120, 45]; they may also be less security-aware, and more likely to divulge passwords or personal information inappropriately. The second type consists of those who don't use IT at all. With the global increase in internet penetration[10] this group is likely to become almost exclusively a subset of the previous group — but there will always be people who choose not to use technology.

Unfortunately the choice not to use technology, or to limit online activities, does not mean that an individual or organisation won't have a digital footprint. It means that the digital footprint will be passive, consisting uniquely of the unmoderated content described by [58].

10 Internet users (per 100 people): `data.worldbank.org`

According to Ambrose, publicly available information is now more visible and has increasing impact and uncontrollable longevity, with harmful content having a longer lifespan [14]. Adapted use of public datasets is done with the implicit consent of the subject (as the data was already in the public domain), thus the user has a lack of control over existing datasets despite a change in availability.

For organisations, rather than individuals, it is even more difficult to manage reputation in public data. For example, local shops who don't see the advantage of having an online presence will still have an entry in the online equivalent of a phone book. They could also be present on Google Streetview[11], on review pages and blogs. If the Streetview image does not show the results of recent urban regeneration, or a restaurant owner cannot distance themselves from reviews pertaining to the previous tenant, this could deter potential customers of non-internet using SSITUs before they even leave home. To quote Ambrose [14]:

> "Old information threatens harsh and wide-reaching consequences to the socially valued and often protected individual interests of reputation, identity, and rehabilitation." [14]

As one participant highlighted, the public profile of a SSITU could contain enough information to make the user vulnerable to confidence tricks or social engineering. In the case of non internet users, they may be more susceptible due to a lack of knowledge of what information is publicly available about them.

Von Solms and van Niekerk suggest that moving from information security to cyber security introduces a moral implication [121]. This leads to the question, *when a data subject has no control over the creation of datasets does system or data control imply responsibility?*

5.3.2.2 *User vulnerability*

Defining vulnerable users within the home IT user group was highlighted as an issue by one participant. This section highlights the context in which any user may become temporarily vulnerable without being an inherently vulnerable user. It is important to highlight user vulnerability in order to avoid defining all SSITUs as vulnerable users.

Users can become vulnerable due to an inability to moderate their online activities sufficiently to mitigate their security risks. Three different sets of user vulnerability emerged from our study:

1. when a user's need to use a service is greater than their need to secure the risk — reputational risk from unmoderated content;

2. when a user lacks the ability to segregate roles within their digital footprint — a too-comprehensive digital footprint enhancing the risk of social engineering, or physical security issues such as stalking, etc.; and

3. when the user's identity motivates attackers to target them (typically being a high-net-worth individual or a public figure) — a greater likelihood of attackers finding and aggregating information to create a more comprehensive digital footprint, as well as a greater motivation to attack.

11 www.google.co.uk/intl/en-GB/streetview/

The first vulnerability can be highlighted by the number of times participants discussed the importance of *pragmatic* decision making where cyber security measures, use of the cloud, or privacy and social media were mentioned. The extent to which online services are now embedded in the way that SSITUs interact, and the lack of influence over the terms of use for these services implied by Wynarczyk et. al.'s description of the constraints of small businesses [129], force users to accept a certain level of business risk.

The example shown in Figure 33(a) shows the owner of a single person company and highlights the inseparability of the participant's personal and public profile described in our dataset. The multi-purpose infrastructures discussed in Section 5.1 also illustrate this problem. For a larger organisation the number of individuals contributing to the core digital footprint increases, but the level of connectivity to personally identifiable information about the employees reduces — often thanks to the requirements of data protection legislation [107]. For example, the questionnaire results indicated that single person companies tend to operate from the owner's home, whereas micro-companies (fewer than 10 people) are far more likely to have dedicated offices. This means that the company's advertised trading address will no longer disclose the home address of an employee.

Digital footprints where an individual's different profiles become entangled increase the risk to that individual's various roles — Workman suggests that, to limit social engineering, risk "commitment to company means withholding commitments from potential threats" [128]. While not all SSITUs are vulnerable, we suggest that there is a higher level of user vulnerability in small organisations, due to the aggregation of different roles within the digital footprint. The amount of personal information about company owners released as a result of this level of integration simply would not happen within larger organisations.

In large organisations c-level executives, often considered to be public figures, might have a more comprehensive digital footprint than other employees. However, this group makes up a very small proportion of the company — especially when compared to a micro-company where half the people working there may be company owners.

In the case of the third vulnerability we identified, these are the users with resources to invest in better security measures and advice to mitigate a far greater risk than the average user. A problem with this was highlighted in one of our case studies — the IT support marketplace is changing. In that case, the participant suggested that the biggest impact that the development of cloud solutions has had is in replacing the IT support role for individuals and micro-companies with preconfigured online services. The participant's customer base has evolved over time so that he is now primarily supporting larger SMEs. He is gradually withdrawing his company's services from those individuals who have not migrated to public cloud services, because, in order to provide high quality support to these individuals, his staff would have to have too much access to the customer's personal information. Having access to the IT system of a high risk user extends the risk to his company. Given the high profile nature of these customers, supporting them is too high a risk to his reputation.

If this pattern was to repeat itself then, even with available capital, individuals with inherently high risk won't be able to source the expertise needed to improve their security — these users would be limited by their knowledge of security and may join the vulnerable user group.

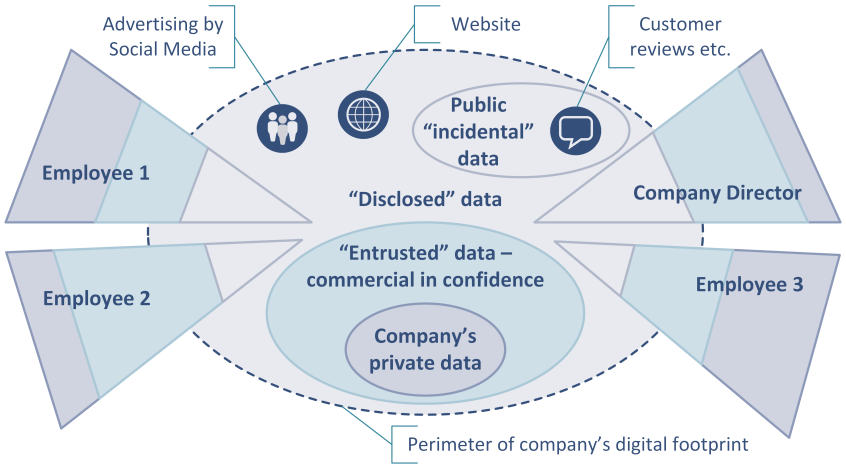


Figure 34: *Analysis fragment: example of how an organisation's digital footprint intersects with its employees'*

5.3.2.3 *Privacy-related decision making*

In the context of this chapter, privacy relates to an individual segregating an element of their digital footprint into a private role, or implementing confidentiality in another role for personal reasons rather than in reaction to a security threat. Measures SSITUs in our dataset take to protect privacy are based on their perceived risk of harm, without significant consideration of security threats.

When considering the cyber security of an organisation the virtual perimeter will include a large proportion of the digital footprints of its employees — both their data and activities — as illustrated in Figure 34. To mitigate security risks, the organisation needs to have visibility of the data and activities they are protecting, but, of course, there are issues pertaining to the ethics of monitoring employees, described for example by Martin and Freeman [60]. One of our participants was reluctant to employ a BYOD model to avoid obvious conflicts of interest between his organisation's need for security and a user's need for privacy. However, when discussing privacy's relationship with security of the individual, the perimeter being secured is far smaller (Figure 31). In this case, our participants implied that the boundaries between confidentiality sought for the sake of privacy and that sought for security become blurred.

The difference is in the motivation for making decisions: is the user attempting to maintain their 'private' role or protect information of value to an attacker?

Participants described their privacy-conscious decision making differently to their security decision making. Adaptations in their online activities included:

- fragmenting service or web use (not displaying customer loyalty);
- adapting or limiting service use (social media, etc.); and
- avoiding linking accounts or using existing accounts for logins elsewhere.

These decisions were intended to reduce the likelihood of unintentional disclosure.

Privacy compromise via aggregation and deduction undermines privacy-conscious decision making, making unintentional disclosure our participants' greatest privacy concern. The availability of public data as open-source intelligence could undermine these practices, compromising privacy via aggregation without any decisions from the

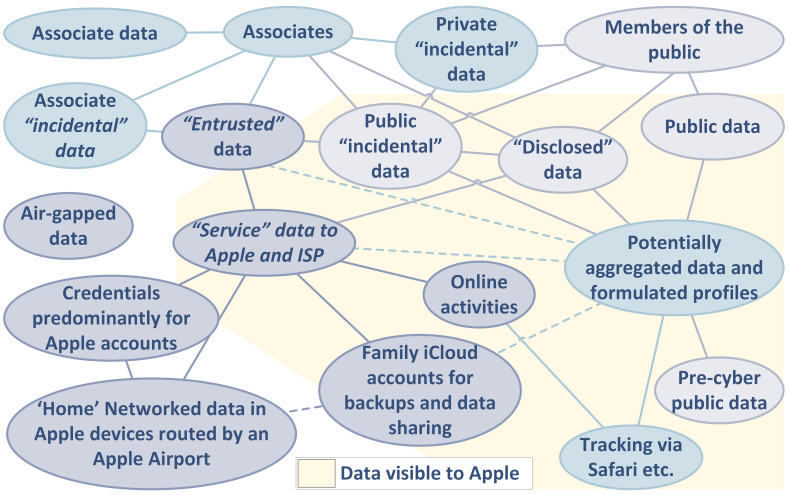


Figure 35: *Data fragment: the digital footprint of a brand-loyal family*

data subject. The ability to de-anonymise public datasets compounds the problem [64, 69, 126].

Participants felt that security would be more comprehensive if as few suppliers as possible were used — one case study described a whole family using only Apple devices and services, with the expectation that this would lead to fewer system vulnerabilities.

Manadhata and Wing describe security's dependence on the attack surface that that user has created [59]; the difficulties SSITUs have in defining their system perimeter was described in Section 5.1. That means that a reduced number of suppliers can qualify as a security decision when service interactions are managed and secured by the supplier. However, a consequence is nominating a single supplier as a *de facto* data custodian — Figure 35 illustrates how much of the family's digital footprint is visible to Apple in our example.

While one of the methods being employed to preserve privacy was the fragmenting of web use and avoidance of account linking, by securing the home system and choosing a single supplier, the participant has provided a complete overview of his and his family's digital footprint to a large corporate entity.

Participants spoke about privacy-compromising decisions and the need for pragmatic cost-benefit analysis. Ultimately SSITUs have to release some information in order to operate; the biggest challenge is to choose how much to share and with whom.

Money can buy better services, but in a data economy service providers are still likely to retain the right to use data, for example [44]. Money can't buy privacy and, as one participant pointed out, some systems — such as some social media services — are designed to be privacy-compromising.

5.3.2.4 *The impact of time on a digital footprint*

The relevance of user control and data aggregation have been discussed in the definition of vulnerable users and user vulnerability. What ties these two factors together is the expectation that a digital footprint will evolve over time as uncontrolled data

is aggregated and augmented, the user's role alters, or the environment changes (the perceived acceptability of a role or position alters).

Users disclose information for all sorts of reasons, ranging from the need to market their company to sharing enough personal information with strangers to arrange a date online. The impact of this on the individuals in our study, in the context of lessening data control and increased aggregation over time, is the rapprochement of cyber security and privacy issues.

Where an individual has the vulnerability of being unable to dissociate their personal profiles from the profile of the company they own, it is understandable that our participants conflate their security and privacy-related decisions. Our data suggests that there are SSITUs for whom security and privacy matters cannot easily be differentiated — what allows larger organisations to apply data protection measures and sufficiently segregate roles to apply access controls is the ability to (perhaps artificially) separate the individuals from the organisation — in a zero-employee company the owner often *is* the organisation.

The participants in this study highlighted examples of where decisions that impact on privacy might create a security requirement over time:

- Where one role needs an online presence for visibility, irrespective of the security requirements of the user's other roles.
- A social media account becomes so valuable for marketing that users lose the ability to step away should they become a victim of trolling or negative reviews.
- Administrators of online accounts could part company with an organisation without handing over control.

The increased visibility of public data and uncontrollable aggregation amplifies this problem: once data is shared it is almost impossible to control.

If the value of the data changes, or it becomes associated with a new role, this could introduce security issues. For example, the association of personal and professional roles could make social engineering more difficult for the user to identify.

The magnitude of interconnections between different profiles makes the smallest organisations the easiest to target: they may have less capital than a large organisation — making large companies with poor security a more appealing target — but, as large organisations improve their security posture (and small organisations are held back by the control they retain of their systems), this situation may evolve.

5.3.3 *The impact of an individual's decisions on other IT users or roles*

The role of associates in a digital footprint was highlighted in Figure 32. There will also be associates who have a greater visibility than initially illustrated, by holding associate credentials for more than one role in a SSITU.

The likelihood of small business owners knowing each other in more than one context is fairly high — in the case study illustrated in Figures 33(a) and 33(b), the participant clearly stated that his company was built by word of mouth. In that case, the participant's role within clubs and charities intentionally intersected with his professional role to act as a form of marketing via corporate social responsibility.

As already discussed, an organisation's digital footprint becomes more complex as it grows — with a corresponding growth in the volume of publicly visible information about employees related to their other roles (unmoderated content over which some control may be negotiated). As an organisation reaches a critical mass security good practice begins to require a separation of roles.

In our example, as well as releasing information that could be harmful to his own reputation, the participant has the ability to influence the reputation of his associates. This implies that an individual's digital footprint can impact an employer, and organisations in partnership can impact each other. These risks are controllable up to a certain point by contract (the supply chain is discussed in Section 5.4), but this does rely on goodwill and can't account for complexity and human error when deciding what information to release — SSITUs rely on their associates to accurately measure the risks defined in Section 5.3.2 when making decisions about what to disclose.

Decisions to change our digital footprints, by using or not using online services, can impact our associates. The complexity of our footprints, the lifespan of data and the number of stakeholders involved make it difficult to determine the implications of any privacy-reducing decision on security. SSITUs have to moderate their online activities in order to mitigate risk created by low-infrastructure systems and highly interconnected supply chains, while their low resources force them to use multi-purpose systems and combine profiles in a way that reduces their ability to limit the growth of their digital footprints.

5.4 System interactions and interconnections in the supply chain

In Section 5.1 we discussed the different infrastructure employed by SSITUs and the prevalence of multi-purpose infrastructures. In Section 5.3 we then highlighted a reliance on contracts to protect the privacy or security decisions made by SSITUs when interacting with associates linked via their digital footprints.

The actors within these systems have different purposes and requirements, and the segregation of roles seen in larger organisations is typically infeasible. These types of infrastructure introduce a cross-pollination of risk between different user roles and organisations: "As soon as information migrates to a device that the company doesn't control, the data is likewise no longer under control" [62].

These types of interaction are a result of a common user, common geography or user association within cyberspace. There are two other types of interaction highlighted by this study: interactions with customers, or with suppliers within the supply chain.

5.4.1 *Supply chain complexity*

All organisations are increasing their use of IT-driven service-based business models [46]. These business models in a supply chain decrease the scope of system control, as supplier-controlled services are often configured for use by unknowledgeable users.

Assets such as data are distributed across the supply chain; in the worst cases, there may be no clear ownership of an asset. Decision making about this system of systems will also be decentralised and, as a result, complexity increases a customer's reliance on a supplier [46]. Bartol suggests that, as a result of this complexity, a "defence in breadth" model is needed to secure the supply chain [15].

Complexity introduces a number of issues for cyber security good practice. One of our RH participants stated that being unable to confidently map the system of stakeholders responsible for the provision of a system introduces complexity into his organisation's security design. End users have an expectation of intuitive systems and devices, which, as highlighted in Section 5.1, can reduce device function in a way that can limit security implementation. One SP stakeholder described how users also expect flexibility in the devices they use, which also limits the scope of security design, despite users expecting adequate security from suppliers. Finally, SSITU system risk owners in our study expect the security of individual components to be adequate, but lack sufficient knowledge to understand how inter-system interactions may be the source of vulnerabilities.

In Section 5.2 we discussed how these design complexities, instigated by the IT-driven business model [46], might introduce safety hazards via security flaws. The same can be said for cyber security risks of non cyber physical systems within the supply chain.

5.4.2 *Interconnections and interactions with customers in the supply chain*

SSITUs showed an increasing number of logical and contractual interactions with third parties within a supply chain. Specialisation and division of labour are making it possible for many of the SSITUs in our study to interact with larger organisations — an SME's customer base was just as likely to involve large organisations as other SSITUs.

Kagermann et al. describe how companies are making increasingly sophisticated use of technology, and this has led to modularisation, specialisation and division of labour [46]. SMEs are not necessarily entering the supply chain as a cost-effective supplier of an existing service — they may be an expert provider or developer of a single aspect of a system. One RH participant indicated that this makes mapping the supply chain and its interdependencies (to evaluate risk) almost impossible for the end customer.

The defence-in-breadth model was developed in response to how vulnerabilities can be introduced at any point in a system life-cycle or the supply chain [15] — penalty notices issued by the UK Information Commissioner's Office included breaches resulting from poor contracting of system transfers between old and new suppliers, as well as in development and implementation processes[12].

Our participant was concerned about how complexity and degrees of separation makes compliance harder to enforce, but complexity also makes organisations more reliant on their supply chains — in [46] it is stated that it is no longer a simple choice to develop a system in-house due to the level of specialised knowledge required. This reliance made security compliance rules unenforceable for our participant — non-compliant suppliers might not be providing anything related to security and the company needs to retain the supplier for business continuity. Contracts representing expected secure behaviours and actively training contractors helped our RH stakeholders, but there is still a need to measure the financial risks of contractor mistakes for security clauses in contracts to be enforced.

12 Action we've taken: ico.org.uk/action-weve-taken/

Although it is important to formally define cyber security responsibilities in any partnership where there is a logical interaction, contracts don't often mention security [89]. This led to our dataset highlighting a number of issues related to due diligence:

- The acquisition of poorly secured organisations could introduce vulnerabilities into a much larger organisation.
- SSITUs often lack the knowledge to ask for the correct terms in a contract, leaving gaps in the services they buy. A common example is web developers who see no reason to take on support contracts: in building a one-off website they have no need to observe the secure coding practices that would allow a site to be securely maintained and updated long term.

Closer logical connections increase the perceived need for security in SMEs; however, by definition, as price-takers [129], small organisations have to operate at a higher level of risk than large organisations. It is their need for lightweight business processes that is reflected in the cyber security measures they take.

Small organisations will never have the same resources available as large organisations; in many cases they are making risky but rational decisions about security provision. What the stakeholder dialogue within our study highlights is a failure in communication between SSITUs and RH stakeholders of their varying risk appetites, which limits larger organisations' abilities to claim responsibility for risk they expect to have transferred.

5.4.2.1 *The use of standards to encourage cyber security good practice*

Faced with the threat of pervasive SME insecurity in the supply chain, some larger organisations mentioned attempting to define acceptable security standards and push these standards down the supply chain. However, risk-based evaluations of SSITUs, based on standards such as ISO 27005 [6] and the good practice relating security measures to a cost-benefit analysis, described for example by [80], will indicate a lower requirement for security *within that small organisation* than other stakeholders in the supply chain may be comfortable with.

Participants in our study gave a number of opinions about the implementation of security standards:

- Security standards are so expensive to implement that it makes accredited suppliers too expensive for SSITUs.
- Information security standards typically cost too much for a small organisation to implement unless cyber security is their core business.
- Maintaining standards is difficult and costly due to changes in equipment specifications over time.
- SSITUs have such limited resources that involvement in slow processes, such as the development of standards, is often infeasible. Their lack of involvement reduces the benefits standards have to smaller organisations.

Yildirim et al. state that SMEs lacking in resource don't comply, but do use available standards for policy development [131]. SSITUs may be benefiting from standards without incurring the expense of becoming accredited.

In Chapter 2 we introduced standards aimed at SSITUs. The focus of Cyber Essentials (according to one government participant) is to reduce an organisation's vulnerability to commodity threats: it is a light-touch standard at the beginning of the security process and can't protect against the targeted threats that are seen in certain supply chains such as the defence sector.

The standard is fairly prescriptive — there is less focus on risk-based decision-making than, for example, in ISO 27005 [6]. This inevitably led to participants highlighting examples where business processes made Cyber Essentials unachievable. An example was offices being required to have boundary firewalls, but on building sites — where the boundary is between a laptop and a USB mobile data dongle — there was nowhere for the firewall to be installed. In its current version, Cyber Essentials also deems security in cloud services to be outside scope, which will have severely limited its influence for a high proportion of the SSITUs participating in our study.

Despite aiming for ease of use, one participant from law enforcement stated how, in his crime prevention activities, SSITUs felt Cyber Essentials was too complex for them to apply.

5.4.2.2 *Disclosure of cyber incidents*

Legal frameworks in the UK provide a number of voluntary and compulsory options for disclosing cyber security incidents. Victims can report a breach via ActionFraud[13] and any security breach sustained by a Data Controller and resulting in personal data being leaked to attackers has to be reported to the Information Commissioner's Office (ICO) [107].

Law enforcement participants displayed a level of frustration in the small numbers of incidents reported to them via ActionFraud. They need the breach data to know where to focus their resources, to the extent that the local force participating in this study had developed a lightweight reporting process for the local community. In contrast, SSITUs showed limited enthusiasm for reporting due to an expectation of inaction: very few actions are taken by local police forces based on ActionFraud reports and business owners in particular saw little advantage in reporting cyber crimes largely for the purpose of generating statistics.

Participants in law enforcement at a national level are developing strategies for notifying the victims of cyber crime. This is a labour-intensive process and so is limited, but it does provide some SSITUs with the information they need to handle a persistent compromise. These notifications are primarily used to encourage collaboration between different members of the supply chain, where they have visibility of attacks affecting other parties.

One government participant suggested that an information sharing platform (CiSP[14]) was the main source of the government's understanding of cyber threats to small organisations. A couple of SSITUs suggested that CiSP was both a good source of a cyber threat snapshot for SMEs and a conduit to authority, credible intelligence and peer support, but the format of information shared requires a level of security expertise that is rare in SMEs. The information-sharing platform requires membership, which makes the users identifiable to the government. Membership also required recommendations

13 Action Fraud — national fraud and cyber crime reporting centre: www.actionfraud.police.uk
14 www.ncsc.gov.uk/cisp

from other members, professional membership organisations or CERT-UK, making the barrier for entry seem high to some SSITUs.

Our participants stated that members tend to share information that includes their identity so that other members can see the data in context. However, much of the information shared is irrelevant to larger organisations as they are likely to have had the information from another source. As their cyber security practices become more advanced and they begin to consider supply chain risks, large organisations may also benefit from understanding the threats faced by SMEs. Threats also tend to be relevant to a broader range of potential victims as exploits lose their value, meaning that SSITUs could benefit more from the information shared.

While large organisations gain little from information sharing, small organisations might feel they don't have enough to share to warrant joining CiSP. However, the dataset shows that SSITUs tend to rely on free peer support and advice from people they know when they are the victim of a cyber attack.

Indirect outcomes of breach reporting are also not providing value to SSITUs — breaches reported by suppliers such as TalkTalk do not provide the opportunity for customers to select a lower risk supplier, as in protecting their share prices, breach victims limit customers' rights to terminate contracts[15]. SSITU interactions with service providers is discussed further in Section 5.4.3.

SSITUs' attitude towards breach reporting was related to the outcome of the report: they typically ask themselves *does reporting a breach return sufficient value to justify an investment of time?* Information sharing was perceived as being about community peer support, whereas reporting was about informing authority. In one case there was no barrier to entry but it is perceived as a conduit to a statistics engine. In the other case there is the conduit to support and authority, but with a high barrier to entry. In order for the UK Government to obtain the data it needs and for SSITUs to obtain both enough intelligence to promote cyber investment and enough support to warrant reporting, the best of both is needed.

5.4.3 *Interconnections and interactions with manufacturers and service providers in the supply chain*

The SSITUs in our study maintain small, but distributed IT infrastructures, with increasingly complex interactions with the supply chain. They need to secure a system of systems or services, such as the one illustrated in Figure 21(d), where no individual system has sufficiently valuable assets to warrant more than basic or free security measures. A consequence is that there is a clear expectation from our participants that security will be embedded for free in any service they employ or device that they buy. There is also an expectation, if not of a transferred or shared liability with a supplier, then at least of free support in the case of an incident. Relatedly, [48] suggests that customers of cloud services expect a supplier to hold some responsibility for security.

In their defintion of SMEs, Wynarczyk et al. describe how negotiating power is related to size [129], meaning that small organisations are at a disadvantage when working with a larger organisation. Unlike the SSITUs of Section 5.4.2, our participants were treated as consumers rather than partners even in business to business transactions.

15 Talktalk restricts fee waivers for ending contracts(2015): www.bbc.co.uk/news/business-34645412

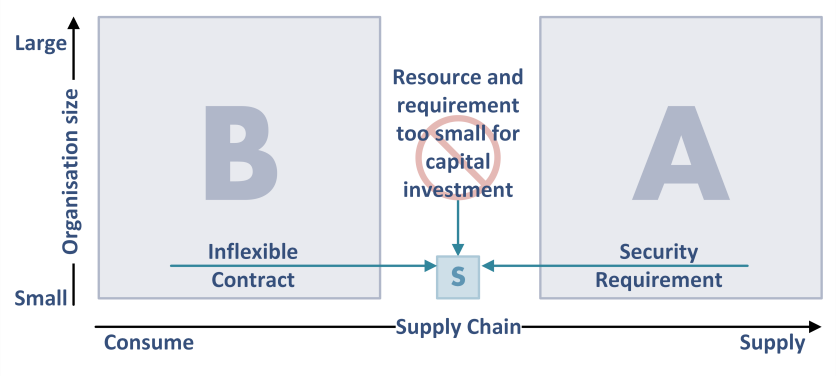


Figure 36: *Analysis fragment: the external pressures experienced by SSITUs in the supply chain*

In terms of security, SSITUs' consumer status resulted in our participants describing only one element where they could influence their own security posture — their password policies. SSITUs in our study found password management difficult, but passwords still remained the main interaction SSITUs had with security in the systems they used. Participants described a variety of means of managing their passwords, including memory techniques, systematic patterns for password creation, retaining soft and hard copies, and using calendar reminders to prompt changes. In some cases, the participants measured the value of the credential before attributing a strong, unique password or reusing their standard password.

Where they were able to influence their own security, the fact that our SSITU participants were able to describe (sometimes convoluted) policies is at odds with our RH stakeholders' opinion that SMEs in particular lacked security awareness. Due to the infrastructure described in Section 5.1 and the lack of influence SSITUs have in negotiating contracts, passwords are often the only adaptable security measure available for them to protect their most valuable assets (with all other measures being controlled by the supply chain).

Security provision in ongoing contracts is also an issue. For example, business to consumer transactions in the telecommunications sector often combine purchasing devices and service provision, in line with [46]'s IT-driven business model. The average length of a mobile service contract is 12–24 months, but manufacturers using Android OS have been criticised for failing to continue updates throughout the lifetime of a handset[16] and the cheaper service contracts include previous-generation devices that may not be supported by the manufacturer for the duration of the contract.

5.4.4 *Distributing security*

Sections 5.4.2 and 5.4.3 described constraints faced by SSITUs in interacting with larger organisations (as both customers and suppliers) to create the infrastructure and accompanying digital footprints introduced earlier. These are summarised in Figure 36, showing how, when combined, it leads to our SSITU participants being squeezed from both sides by the requirements of the larger organisations they interact with, further limiting the scope they have to adapt and make their own security decisions.

16 US government probes mobile phone industry over the sad state of security updates: `arstechnica.co.uk/security/2016/05/ftc-fcc-mobile-phone-security-updates`

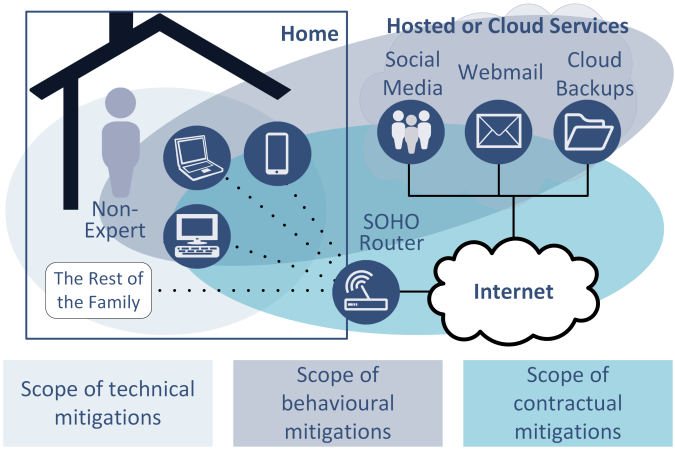


Figure 37: *Overview used to triangulate findings: the available scope of cyber security mitigation when including contractual mitigations within the supply chain*

Larger organisations, in the form of both RH and SP stakeholders, appear to be attempting to deal with security issues within the supply chain by measuring responsibility and transferring risk — which, with organisations of an equivalent size acting in a comparable manner, may achieve stronger inter-organisational partnerships.

The reality of the infrastructure highlighted in Section 5.1, combined with the increased importance of managing their online activities discussed in Section 5.3, creates a system with so little flexibility that, despite having justified security and being pressured or advised by the supply chain, our SSITUs would see minimal benefit from investment in cyber security.

In the supply chain of Figure 36 the organisation with the most power to reduce the risk of organisations A and S is organisation B — the large supplier of the SSITU. Some improvements may be made by the most influential member of the supply chain using that influence to encourage more widespread changes, as described by [99]. However, the 'most influential' member of the supply chain may not be the RH stakeholder — Egloff describes how technology companies are have become so large that they now assume "sovereign-like functions" [30] — RH stakeholders may be unable to influence the decisions of the inadvertently SP but risk-transferring technology providers represented by company B.

Company A may be able to reduce their risk in supply chains where SSITUs interact with other SSITUs, by a combination of encouraging standards and increasing the availability of affordable accredited services. However, the risks related to the interaction of systems maintained by different parties, the blurred responsibilities of system stakeholders at these interfaces described by [53] and the characteristic low resources of SSITUs, will still limit results. We suggest that RH stakeholders may have to work in closer partnership with SSITUs to establish where there may be attack vectors the SSITUs are unable to block.

As can be seen in Figure 37, by finding a way to include the supply chain when making cyber security decisions, the scope of mitigation available to SSITUs expands once more. Only allowing cyber security decisions that influence any of the three system elements — technical infrastructure, digital footprint and supply chain — can SSITUs get close to implementing defence-in-depth or defence-in-breadth.

This chapter, in conjunction with Chapter 4, has reported the results of our UK case study on small-scale cyber security. We have illustrated how, once a SSITU has justified investing in security, the choices they make will be constrained by a broad number of limitations existing in the systems and community they operate within. These are as follows:

- micro organisations (and low-infrastructure organisations above that size) tend only to apply basic security measures — they do not have many of the elements of large corporate IT systems that the more advanced measures are designed for.
- SSITUs implement extremely distributed systems with a large number of contracted services, making defining a perimeter for security challenging.
- SSITUs often operate in shared infrastructure, further limiting their control.
- Due to the size of SSITUs' core systems and the volume of services they consume, the digital footprint becomes more relevant to security than in a larger organisation.
- SSITUs are more likely to have linked their personal and professional roles in their digital footprints, potentially making both the individual and the organisation vulnerable.
- RH stakeholders attempt to increase the security of SSITUs in the supply chain using standards to mitigate their own risk. They are also beginning to recognise safety-related cyber risk in adjacent SSITU systems that SSITUs are as-yet unaware of.
- SP stakeholders attempt to simultaneously limit their liability and retain control of the system in an attempt to reduce their cyber risk and protect profits.
- As 'price-takers' [129] SSITUs experience insufficient flexibility in their interactions in the supply chain to influence overall security.

In introducing this chapter we asked the question *Once a SSITU has justified investing in cyber security, what constraints within their IT system limit their decisions?* In response we have shown that the constraints are numerous and complex, but that small-scale cyber security infrastructure is not just about technology. There is a need to consider technology use in context of interactions within a broader ecosystem of a supply chain, users with multiple roles and the impact of the digital footprint on security.

In the Chapter 6 we combine the results of our case study with the more general understanding of cyber security, privacy and safety best practices discussed in Chapter 2 to develop a requirements framework for small-scale cyber security.

6

DEFINING A SMALL-SCALE CYBER SECURITY REQUIREMENTS FRAMEWORK

The scope and complexity of designing cyber security solutions for SSITUs motivated the survey presented in Chapters 4 and 5. To complete the research, this chapter responds to research question 4 presented in Chapter 1: *How can understanding the context that SSITUs operate within assist in the development of a small-scale cyber security requirements framework?*

We generalise the outcomes of our survey as the basis for developing a requirements framework for small-scale cyber security. The intention is to increase the usability of these research outcomes, by providing them in a format that can be directly adopted in the development of tools and initiatives for the sector, whether initiated by SSITU stakeholders or from the broader scope of the supply chain. Linking the requirements framework to current best practices also initiates the development of a less divisive approach to cyber security best practices that may eventually allow organisations of different sizes to interact more efficiently within the supply chain.

As this chapter re-evaluates the findings of previous chapters with a specific purpose in mind, all phenomena were considered (the full coding summary can be found in Chapter 3's Table 3).

Section 6.1 discusses the approaches that have been taken by cyber security practitioners until now, with a comparative overview of the attributes of the small-scale cyber security ecosystem our survey provided. The requirements framework is described in Section 6.2, with additional supply chain requirements outlined in Section 6.3. Section 6.4 summarises the chapter.

This chapter is based on [74].

6.1 WHAT IS THE CYBER SECURITY PROBLEM TO BE SOLVED?

6.1.1 *Stakeholders*

An aspect of the dialogue around cyber security for small organisations is the number and variety of stakeholders. In Chapter 2 we defined three (not mutually exclusive) stakeholder groups — SSITUs, security providers (SPs) and risk holders (RHs).

In identifying and differentiating between these stakeholder groups the survey was able to identify discrepancies in the goals these stakeholders have, as well as issues in problem ownership and gaps in experts' knowledge of the SSITU sector.

An outcome of these concerns (described in Chapter 4) is that it is not uncommon for project sponsors from the RH group to task members of the SP group (often those SPs most familiar with implementing security in large RH organisations) with the development of cyber security solutions for SSITUs. The lack of engagement from SSITUs is read as a lack of awareness (and so a total lack of implementation of) cyber security.

This becomes problematic when attempting to define cyber security requirements for SSITUs. Robertson and Robertson define *the sponsor* as the person who 'owns' the project, paying for, and so having final say over, the product. *The customer* is defined as the 'new owner' — who will have to find the product "valuable and useful and pleasurable" if they are to be persuaded to buy it [90]. (The distribution of sponsor and customer roles between stakeholders is discussed later in the section.)

Both sponsors and customers have the ability to influence requirements, however, it is unusual for the motivation of the sponsor to conflict so categorically with a customer's constraints in the way that our survey suggests. The discussion becomes about the problem security practitioners think they are trying to solve, versus the problem our data implies SSITUs are attempting to solve.

As stated in Chapter 3, requirements exist whether they are identified or not, meaning that this polarisation of requirements may have had a significant contribution to the lack of progress in securing the SSITU sector.

The root of this problem seems to be a disparity of expectations created by the realities of implementing cyber security in two very different environments.

Another issue that emerged from the survey was how cyber security becomes embedded in other services, which leads to some SSITUs inadvertently becoming SPs. An example is a small innovation centre that provides infrastructure (including internet connections and networked printers) to micro-companies, that had become their customers' source of both network security measures and advice. They had to implement security above and beyond their contractual requirements as a result of customers blaming them for incidents caused by poor endpoint security.

Where larger organisations may become SPs and be encouraged to improve their product (or the security embedded in their product) by their customers or by RHs, SSITUs as SPs may have limited experience or scope for employing experts with which to make decisions. However, this does imply that SSITUs may more directly influence the security of other organisations than scenarios involving the mishandling of login credentials might suggest[1].

In conjunction with the results the empirical study described in Chapters 4 and 5, Section 6.1.2 explores how the definitions of cyber security best practices discussed in Chapter 2 make assumptions about the systems they will be applied to and the difficulties this poses for SSITUs. The section then goes on to discuss the maturity of SSITU cyber security practices in our survey and, finally, how these issues frame the problem that a requirements framework might begin to address (Section 6.1.3).

6.1.2 *Aligning with cyber security best practices*

What is evident from the description of cyber security principles discussed in Chapter 2, is that, owing to the assumptions made by cyber security experts, cyber security 'best practices' are in fact the cyber security practices best adapted to large mature organisations who have a large amount of fixed infrastructure.

1 Using the example of the Target data breach [84].

Examples of these assumptions that can be extrapolated from the five categories of cyber security principles illustrated in Figure 5 (presented in Chapter 2) include:

- Category 1: an assumption that the organisation has sufficient understanding of the provision of their IT system to identify key stakeholders.
- Category 2: an assumption that a cyber security function can reach a critical mass, based on an expectation that other business functions are formalised, documented and of a comparable magnitude, and an assumption that it is possible to identify all the relevant assets and their location within the organisation.
- Category 3: an assumption of the availability of knowledge and human resources capable of assessing cyber security risk, as well as an assumption that equivalent risks and investments have been documented across the company.
- Category 4: an assumption that the organisation has ownership of its IT infrastructure or influence over the terms of contracts, has a dedicated physical environment, has sufficiently formalised processes to implement a coherent user policy and access controls, and has a minimum level of financial or human resource to fulfil a broad range of technical roles potentially 24/7/365.
- Category 5: an assumption that the organisation's business processes are sufficiently adaptable to sustain continuous evolution of processes, and that there is sufficient resource to test alternatives once the organisation has invested in a solution.

A number of these assumptions — the existence/importance of stakeholders, the documentation of assets and an expectation of adaptability — are equally challenging for any size of organisation, but they persist due either to a need to define the problem to be addressed, or to acknowledge threat actors' abilities to fundamentally change the operational environment. In the case of adaptability, smaller organisations have been found to have an advantage, although this is usually outweighed by their inability to afford to test multiple options before implementing a system [52].

However, the survey indicated that the level of outsourcing and bring your own device (BYOD) models made category 1 challenging despite an organisation's limited size. Categories 2–4 were challenging as in organisations of fewer than 25 people there was unlikely to be any dedicated IT function and no SSITU participant described a dedicated cyber security function. The smallest SSITUs lack the knowledge and time to develop coherent cyber security processes (that would be far more formal than any other process inside of the organisation) and lack the resources to employ an expert.

Category 4 is also more challenging due to the highly distributed nature of the majority of SSITUs' IT systems — they lack a minimum number of employees to fulfil key security roles, the system or device ownership, the physical access, or any dedicated office space and dedicated (and so formalised) roles. They have conflicts of interest due to the combination of roles each individual has and due to the multi-purpose use of many of the devices used within the organisation. Their systems are typically so distributed that there are not enough layers to be able to implement defence-in-depth and, as small organisations, a lack of influence over suppliers precludes the implementation of defence-in-breadth. In some contexts they fail to even implement the measures required by Cyber Essentials due to a lack of controlled infrastructure.

Category 5 is challenging as non-technical decision makers tend to invest with the expectation of having adequately handled the cyber security challenge. While decision makers in any organisation — no matter the size — will not want to continually reinvest, in large organisations a defined IT or cyber security function would partially own the cyber security risk and so maintain both knowledge and the pressure to invest. When SSITUs' decision makers have the responsibility to maintain their own knowledge of the threat landscape, and faced with severely limited budgets, they are more likely to assume that the cyber security problem has been adequately 'solved'.

The closer a SSITU's IT system gets to that of an individual working from home, the more difficult it becomes to find the equivalent process or equipment to apply security best practices to. It is for this reason, balancing knowledge, the way processes are carried out by SSITUs and existing security measures that apply to the type of IT systems they operate, that Cyber Essentials is less comprehensive than other descriptions of best practice (with only category 4 measures, as stated in Chapter 2). However, the survey also highlighted the importance of both reputation and the associated risk that personal data breaches pose to smaller organisations in motivating SSITUs to engage with cyber security. Although Cyber Essentials addresses certain threats deemed to be present for all IT users, it does not link the application of security measures to perceived risk in a way that SSITUs could use to justify and document their security decisions for the GDPR.

The proportion of cyber security principles illustrated in Figure 5 typically implemented by SSITUs indicates that the maturity of cyber security practices in small organisations is comparably low. However, if the measure of maturity is taken against the proportion of principles *achievable* by a small organisation, or what they achieve given their budgets, then SSITUs have a more mature approach to cyber security than many of the larger organisations they interact with. Unfortunately the complexity of the environment within which they operate and the availability of achievable security mechanisms increases the asymmetry present between attacker and target. A lack of achievable security processes does not correlate with a lack of potential attack vectors.

Although this has been highlighted as a concern to the RH stakeholder group earlier in this chapter, due to their interaction in the supply chain, it is also of concern to larger organisations for another reason. One business model highlighted in Chapter 5 was that of a low-infrastructure organisation — while it was difficult for small organisations with traditional business models to avoid introducing fixed infrastructure above a certain size, it was possible for SSITUs to grow far larger using non-traditional business models with large numbers of employees working from home or on customer sites. In these instances the organisations did not increase their control over the IT system and so were not able to transition towards cyber security best practices as the organisation grew. Low-infrastructure IT models bring the infrastructure of large organisations closer to that of small organisations — as large organisations migrate towards cloud services they begin to encounter similar security issues to those currently faced by SSITUs. While influence and financial standing may resolve some of these issues, there are benefits to the wider supply chain in adapting security principles to a more distributed IT model.

The inaccuracies in the assumptions made about small businesses highlighted in this section demonstrate why Robertson and Roberston's recommendation that the trawl

for knowledge be technology-agnostic [90] is so relevant to the development of security requirements for SSITUs.

6.1.3 *Framing problems as requirements*

There is a security gap between the SSITU stakeholder group and larger RH stakeholders, assuming that both follow the relevant guidelines for implementing security (Cyber Essentials and ISO 27001, etc. respectively), due to the focus on the application category for SSITU solutions. The size of the gap makes transition from SSITU processes to a larger corporate model of security challenging, especially given the difficulty some survey participants expressed in implementing essential measures. The survey indicated that SSITUs could only make the business case to transition to more expensive corporate cyber security practices where cyber security was a core product or service they supplied to their customers.

The challenge for a large proportion of SSITUs is to find the business case to transition towards *essential* security measures. By contrast, the essentials many SSITUs are aiming for is not enough to reduce the risk imposed on RH stakeholders in the supply chain. With the GDPR being one of the key motivations for engaging with cyber security there is a need for SSITUs to implement more than the essentials — the GDPR's principles are distributed across the five categories and so the needs of SSITUs are broader than the recommendations of Cyber Essentials. The big difference is that, even where increasing the scope of their cyber security needs, SSITUs will not be able to assume responsibility for the magnitude of risk some of the RH stakeholders wish them to mitigate against — SSITUs will only ever be able justify investing in security in proportion to their internal risks and annual turnover.

Ultimately the dialogue around SSITUs and cyber security is attempting to solve two separate problems:

1. achieving a basic level of engagement with cyber security from all SSITUs — either implementing advised 'essentials' or complying with regulatory requirements; and

2. transitioning SSITUs from the bare essentials towards more advanced best practices to align their cyber security capability with other members of the supply chain.

The first problem, despite the UK Government taking some ownership as an attempt to protect the economy as a whole, assists in mapping out *SSITU cyber security requirements*. It becomes more difficult for SSITUs to justify their engagement with the second problem: it maps the needs of RH stakeholders, but in the correct context could serve to reduce the capability gap between small and large organisations to a point where more collaborative security processes could be feasible. For this increase in scope of security 'essentials' across the remainder of the five categories of principles to occur, the goal of 'best practices' has to be expressed without the assumptions that render them unachievable for SSITUs. Referencing Figure 5 and ISO 27001, Figure 38 illustrates how the five categories of cyber security principle might be summarised in both

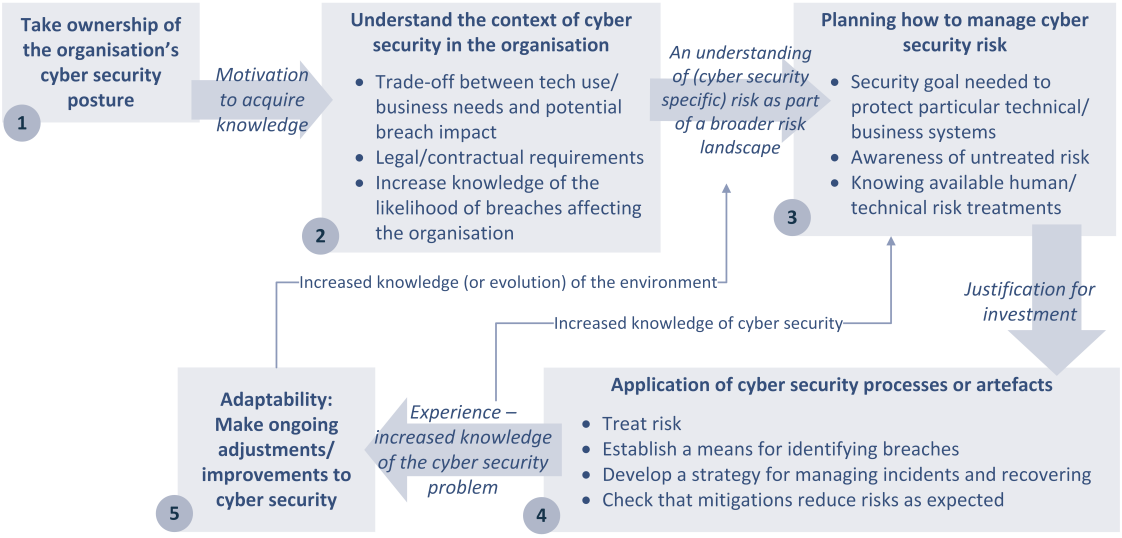


Figure 38: *A technology and business process agnostic description of cyber security best practices*

a technology and business process agnostic way, producing the "essence of the work" [90] cyber security best practice is attempting to achieve[2].

The five categories of cyber security principle can be summarised as follows:

1. Ownership
2. Context
3. Planning
4. Application
5. Adaptability

These categories tie into the elements of the requirements engineering process described in Chapter 3, which will be used in Sections 6.2 and 6.3 to create the framework. An overview of the requirements engineering process described in Chapter 3 and used in Sections 6.2 and 6.3 can be seen in Figure 39. The five categories can also be used in conjunction with the template provided by [90] to assist in evaluating the resulting framework.

1. A decision maker's perception of problem ownership defines the goal and scoping;
2. the business context provides the scenario (including global business constraints) and provides an enriched understanding of threats/vulnerabilities, etc. to that system, which feed into an understanding of risk;
3. planning describes the translation of ownership and business context to system security requirements;

2 The description of the essence of the work needs to be both technology and business process agnostic to align with the goal described in Chapter 3 for the trawl for knowledge to be unbiased by *security solutions*, which can be both technological and procedural.

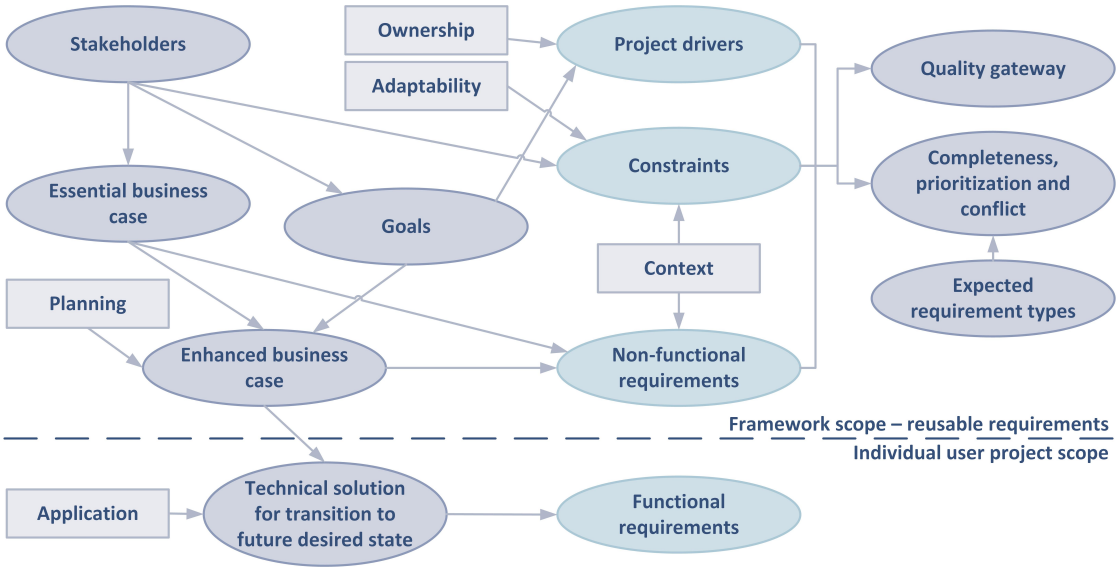


Figure 39: *An overview of the elements of the Volere requirements engineering process used in this paper*

4. application includes some global system constraints (although the majority of the application requirements are out of scope for the framework, as they relate directly to the solution a framework user might develop); and

5. a SSITU's adaptability relies on the availability of suitable[3] solutions *in combination with* the decision maker's ongoing cyber security experience and the information supplied both by the system and about new security solutions. Adaptability implies a need to regard security as an ongoing process rather than an atomic task.

6.2 A CYBER SECURITY REQUIREMENTS FRAMEWORK FOR SSITUS

The presentation of the cyber security requirements framework for SSITUs provided in this section begins by outlining its stakeholders and goals (Section 6.2.1), with Section 6.2.2 describing the essential business case. Section 6.2.3 discusses the resulting requirements (which can be found in full in Appendix D) and Section 6.2.4 evaluates the requirements against the validation criteria described in Chapter 3.

6.2.1 *Stakeholders and their goals*

All three stakeholder groups discussed in Section 6.1 contribute to this requirements framework. However, this framework envisages SSITUs as the intended customer (requirement 10002) and an eventual SP (which may also be a SSITU) as the project owner (10001). Risk holders and pre-existing SPs will play a limited role as adjacent system owners, introducing constraints that may limit the scope described by the customer,

3 With the level of usability, lack of disruption, and adherence to budgetary constraints described by the framework's context requirements.

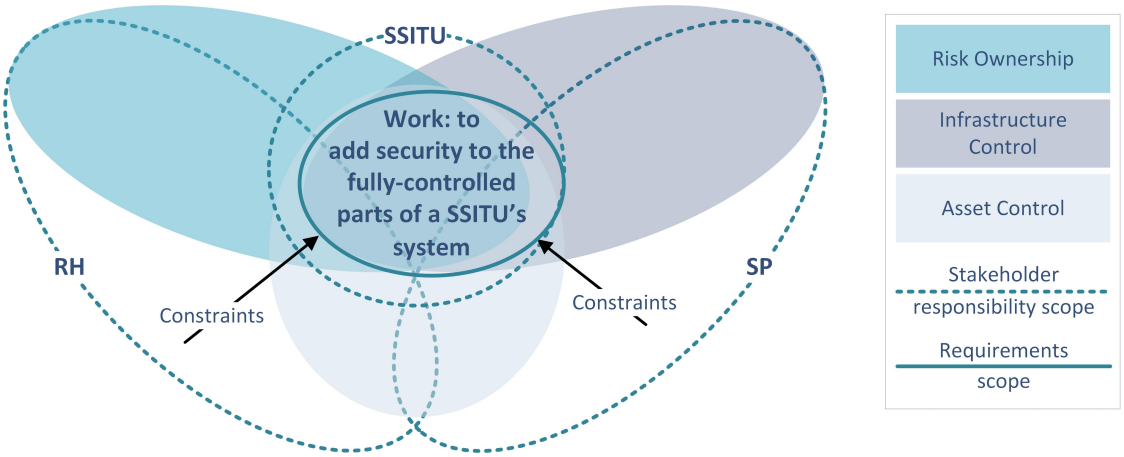


Figure 40: *Context diagram for the requirements framework for SSITUs*

but without the authority to introduce requirements of their own. The SSITU's goal is to reduce their own cyber security risk (problem 1 in Section 6.1 — 11101).

6.2.2 *Essential business case*

As described in Chapter 3 the essential business case outlines an abstracted, technology-agnostic version of the problem to be solved alongside a scenario that provides business context.

6.2.2.1 *Context diagram and framework scope*

The customer is a SSITU that has both recognised cyber security as a risk and taken ownership of the problem.

The decisions they make about cyber security, as outlined in Chapter 4, will be proportionate to the risks faced uniquely by that organisation and their ability (given their level of knowledge and resource) to reduce those risks. They will predominantly focus their investment on assets they fully manage — they control the data assets, own the infrastructure and cyber security related to those assets poses a *direct* risk to their organisation. This is highlighted by how the requirements scope intersects with these elements in the context diagram shown in Figure 40.

They are aware of reputational risk produced by adjacent systems and the risks associated with uncontrolled assets (such as those controlled by SPs), but will only invest in measures that protect assets they have an unambiguous responsibility for (including data protected by the GDPR). As Figure 40 illustrates, a large portion of infrastructure ownership and asset control falls outside of the SSITU's responsibility, controlled by the SPs. The RHs' responsibilities include a large portion of the risk ownership and asset control. Both of these issues mimic the findings of Chapters 4 and 5, which highlight that this lack of control is a significant source of constraints, for example, their limited rights in SP contracts and the limited ability to negotiate the mode of interaction SSITUs have with RHs.

The requirements scope encompasses a small amount of infrastructure not owned by the SSITU and some assets not under the control of the SSITU. The former is to encompass the small number of SPs a SSITU would have some influence over, for ex-

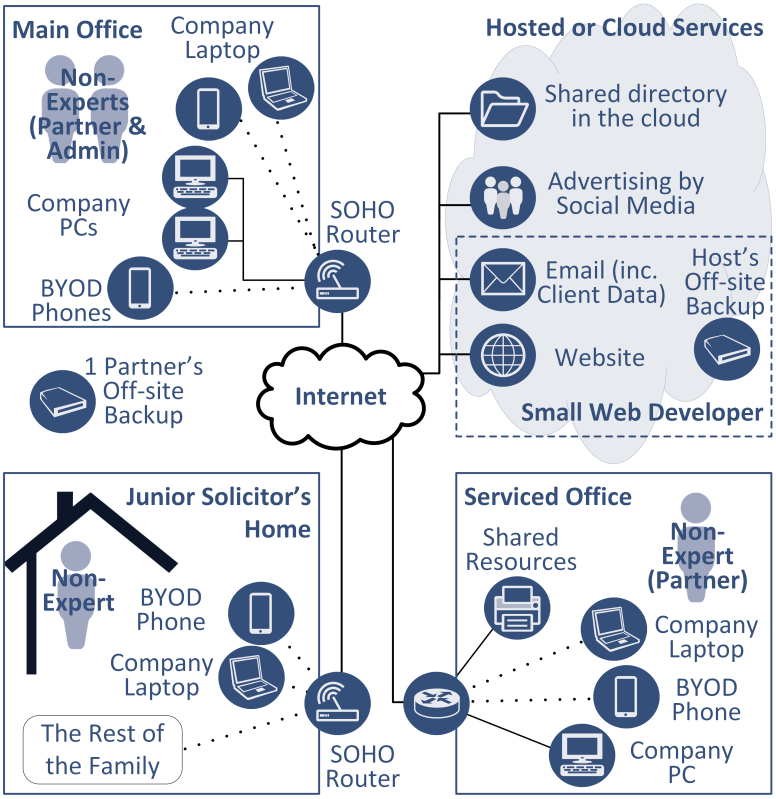


Figure 41: *SSITU framework scenario architecture*

ample, the business owner's employees discussed in Chapter 4. The latter is to handle the proportion of SSITUs' most valuable assets, represented by credentials for third party services, which were discussed in Chapter 5.

6.2.2.2 *Sample scenario*

The following scenario is intended to support framework users in understanding the scope we have used in developing our requirements and to facilitate our discussions in Sections 6.2.3 and 6.2.4. As with the scenarios used in Chapter 4 and Appendix B, this scenario is based on real-life examples and components of our dataset, without representing one specific participant.

The scenario uses the example of a small legal firm that has two directors, a junior solicitor and a part-time administrator. The firm provides a mixture of legal services, from writing contracts to representing their clients in criminal cases, as well as one director volunteering as in-house counsel for three small charities. They have a main office, where one partner works every day, alongside their administrator. The office has a spare meeting room, used by either of the other solicitors when they want to see clients from that location. However, as the other two solicitors are based some distance from the main office, one works mainly from their home and the other runs a small 'branch' from a serviced office.

All members of the company are issued with IT equipment — the two partners have desktop and laptop computers, the third solicitor uses only a laptop and the administrator has a PC in the main office. All three solicitors use their personal smartphones

to check emails and talk to clients. The administrator answers the landline when they are in the office.

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. Due to the size of the main office there is very little fixed infrastructure: the business relies on small office/home office (SOHO) routing. In the serviced office the company has no control over the infrastructure, which they access via WiFi to connect to the Internet and shared resources such as printers.

All data held by the company is covered by UK data protection law, or is held commercially in confidence in line with the solicitors' professional ethics body.

Due to the company's distributed offices and the need for the solicitors to collaborate, the majority of the solicitors' records are held (and automatically backed up) by a cloud service provider, who also enables all staff to access the documents they require. Only one partner remembers to regularly backup the files held on his PC onto an external drive; the other employees are inadvertently relying on local copies of their documents should the cloud service be unavailable or become corrupted.

A large proportion of communications between solicitors' offices or to clients are still using hard copies due to the need for original documents. Specialist couriers are used for the most sensitive documents. However, during negotiations, etc., these documents are now extensively exchanged via email before they are signed. Customers also regularly send sensitive information by email. A network diagram illustrating the environment is given in Figure 41.

6.2.3 *Requirements*

The requirements fall into eleven inter-related themes, which connect to the five categories of cyber security principle discussed in Section 6.1 as follows:

- Ownership
  - Reputation as an incentive to secure
  - Scoping responsibility
- Context
  - SSITU system differentiators
  - SSITU self-efficacy
  - The prioritisation of business continuity
  - SSITU digital footprints
  - SSITUs' lack of influence
- Planning and Application (combined)
  - Multi-purpose system constraints
  - System distribution constraints
  - GDPR compliance requirements

  - (Continuity, self-efficacy, digital footprint and system requirements derived from the preceding constraints)

- Adaptability
  - Evidence-based security

6.2.3.1 *Ownership*

By far the greatest cyber security incentive described by SSITUs was the need to protect reputation. It is this, above all else, that is driving SMEs to take ownership of the problem, that concerns individuals faced with the uncertainty of having their identity stolen, and pushes charities and small clubs to limit their online activities.

The reason for this is highlighted by the two main constraints related to reputation (summarised in Table 10): that incidents impacting on reputation are likely to be *catastrophic* for SSITUs (11106); and that SMEs must comply with the GDPR, or exempt SSITU organisations often need to align themselves with the GDPR (11132).

SSITUs' concern about the threat of reputational damage as a consequence of a data breach is twofold: the rationale for stating that reputational damage would be catastrophic is that *SSITUs lack the financial resilience of larger companies* (10009). As described in Chapter 4, SSITUs lack the influence to hold a larger organisation to a contract in the aftermath of a breach and our solicitor would struggle to retain clients should their confidential information be leaked. The constraints scoping cyber security responsibility (also in Table 10) highlight the other issue SSITUs face in attempting to take ownership of their cyber security problems. SSITUs are being encouraged to take ownership of the cyber security *risk*, while the ecosystem limits any ownership they may have of the systems themselves. This becomes evident when comparing our scenario architecture (Figure 41) with the decision-maker controlled elements of a system discussed in Chapter 4 (Figure 13).

This scenario leads to the conflicting expectations that SPs' responsibility extends to support (11111), with the extremely narrow scope of responsibility SPs are taking for SSITU security (11129, 11134, 11144, 11133) and the limited legal protection offered by legislation (11131, 11143). For the most part SSITUs are limited to best-effort quality of service. This imbalance is a recurring theme throughout the context and planning and application elements of the framework.

For the individuals described in Chapter 5, who find it impossible to differentiate professional and personal roles, there is a second recurring theme. They are simultaneously individuals who are required to achieve GDPR compliance, and individuals who cannot sufficiently divide their professional and personal activities to ensure that their own personal data is protected by the same legislation (12212). In our sample scenario, the solicitor working from home and volunteering as in-house counsel would face these issues. They are required to take ownership of a problem for others that they are unable to resolve for themselves. This scenario conflicts with the context of SSITUs needing to preserve their self-efficacy (10005) and SSITUs' relationship with data protection becomes another recurring theme across the framework.

There are also a number of requirements related to problem ownership stated in the framework, for example, SSITUs need incentives to implement security (11142), and accountability (such as that promoted by the GDPR) as a catalyst for evolving formal processes (10003). SP stakeholders have a responsibility to reduce the effort required

RID	Description	P	Conflicts
11106	Incidents impacting on reputation are likely to be catastrophic for SSITUs	X	
11132	SMEs must comply with GDPR and exempt SSITU organisations often need to align themselves with GDPR	X	12251
11129	SSITUs have no influence over SLA/contract terms.	X	12251
11131	Commercial SSITUs are treated as consumers	X	
11143	GDPR only protects (living) individuals in a personal context, not all customers SPs consider 'consumers'	X	11131, 12212
11133	SSITUs' main service provider may also be a novice (network infrastructure)	X	11111
11134	SSITUs lack ability to stop other system stakeholders altering configurations without permission	X	
11144	SSITUs' most valuable digital assets may be credentials for 3rd party services	X	11129
11111	SSITUs make decisions based on the expectation of supported services	X	11124, 11133

Table 10: *Ownership constraints*

for SSITUs to engage with cyber security (10004), which aligns with the comments made by Herley [42].

The fit criteria for this set of requirements state that a solution should support GDPR compliance and is: a default setting; can be achieved and maintained by novices; or it becomes one of the security measures *SSITUs* consider a benchmark requirement for reasonable cyber security.

6.2.3.2 *Context*

The operational context of SSITUs, when compared to that of a large organisation is markedly different. This difference can be observed in the comparison of our scenario architecture (Figure 41) with an example of the type of system architecture a large organisation might begin with — as per Figure 42.

As mentioned in Section 6.1, assumptions about the system and operational context underpin the majority of cyber security best practices. Table 11 describes the constraints these differences in both systems and organisational processes impose on solution designers. The system constraints revolve around the lack of artefacts (such as servers and network infrastructure, present in Figure 42) that security measures could be applied to (11139), alongside issues justifying investment in this type of security measure (and the associated infrastructure) in an organisation of this size (11140, 11138, 11115). The different roles one SSITU may have also creates such a complex digital footprint that access control becomes challenging (11141). The counter to these constraints describe how SSITUs' socio-technical processes are too informal to support rigid cyber security process (11109) — cyber security best practice does not align with other SSITU processes. These organisations also don't document their processes (11117), despite being IT-dependent (11135), and will prioritise business continuity over security, even when accepting new contracts (11107, 11136).

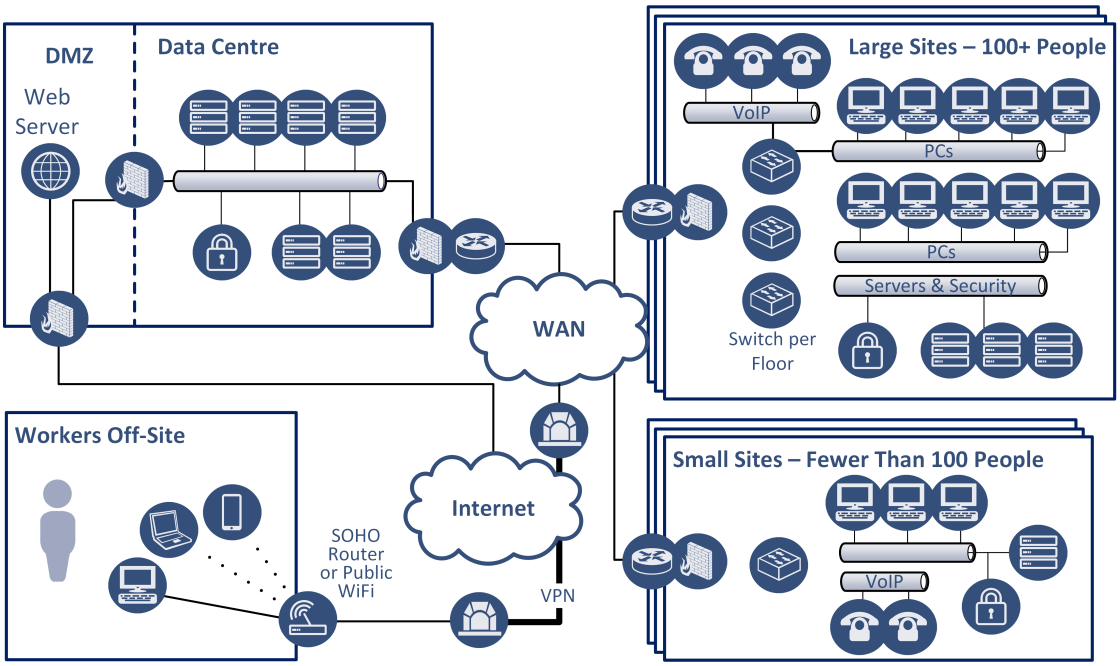


Figure 42: *Example large organisation architecture*

RID	Description	P	Conflicts
11139	SSITU systems lack the artefacts many security measures are designed to protect	X	11132
11138	SSITUs lack the critical mass to protect their highest-value assets	X	11132
11140	SSITUs' assets are not of sufficient value to warrant security investment	X	11132
11115	SSITUs use consumer devices or solutions in a business setting	X	13315
11141	SSITUs often have detailed, interconnected and non-reducible digital footprints	X	
11109	SSITU organisational culture may be too informal to support rigid security processes	X	11132
11117	SSITUs' socio-technical processes will be undocumented	X	11132
11135	SSITUs are IT-dependent	X	
11107	SSITUs' day to day operation takes precedence over administrative/ housekeeping processes	X	11132 + 11106
11136	SMEs have to accept risks where a security requirement stops business functioning (including by limiting their ability to accept contracts)	X	11132

Table 11: *SSITU system differentiators and the prioritisation of business continuity*

It is worth noting how many of these constraints are in direct conflict with requirement 11132 — compliance with the GDPR. This is as a result of planning and application constraints 12251 and 12248 — the GDPR adopts the assumptions made by cyber security standards, and standards make technology-specific assumptions about the system they are being applied to.

The constraint of needing to remain operational irrespective of the security risk this poses (11107) is the biggest barrier to improving security, as it encompasses small-organisational issues from cash flow to influence over contracts. 11107 is in direct conflict with what we have identified as the two main incentives for SSITUs to take ownership of security (11106 and 11132).

These constraints result in the following solution fit criteria: solutions are usable by individuals in a home environment and do not suggest that SSITUs cease to carry out any activity. SSITUs' own security and privacy processes are preserved by ensuring that solutions: do not introduce additional personal information into the public domain; reduce the amount of aggregated personal information; or remove personal information from the public domain.

The theme of self-efficacy also plays a major role in securing SSITUs. As noted in preceding chapters, there has been an observed improvement in SSITUs' awareness of cyber security. However, this knowledge does not necessarily translate into increased insight as a cyber security decision maker (10007). In our scenario it is the company directors who will make decisions about cyber security — as solicitors they may have a good understanding of data protection legislation, but this does not provide them with the complementary technical experience required to choose and implement a solution. This scenario is combined with the lack of available SSITU cyber security expertise and an inequality in the level of support offered (11103, 11104, 11105).

This results in two clear and high-priority requirements. First, maintaining self-efficacy is a delicate balance and SSITUs need to feel less vulnerable to retain their independence (10005). Secondly, there needs to be a chance of efficacy — investing in cyber security needs to result in sufficient risk reduction that a *catastrophic* breach ceases to be inevitable (10006). These tie into themes around influence shown in Table 13, in the planning and application category, as well as relating back to the need for SPs to take responsibility for reducing SSITUs security burden (10004). To summarise, SSITUs can't afford to employ experts (11121), there are limited experts available (11103), SPs don't want to offer SSITUs high-end support (11124), and the small-scale cyber security ecosystem can't afford to protect and support SSITUs who have lost their self-efficacy at scale (11105).

The self-efficacy requirements result in the following fit criteria:

- Solutions are implementable by novices.
- The solution is presented to the SSITU in a way that makes them certain that it will have a measured effect and they can easily implement it.
- There is a combination of solutions that allow SSITUs to comply with the most reputationally damaging of: the GDPR; or customers' cyber security expectations.

Following on from the issues raised under the theme of ownership (11129, 11131), Table 13 provides some examples of how SSITUs' lack of influence constrains the cyber security solutions available to them. These constraints range from a lack of influence

RID	Description	P	Conflicts
10007	SSITUs are security aware but lack equivalent knowledge as decision makers	X	
11104	SSITUs have inconsistent access to cyber security knowledge	X	
11105	There is less legal support available for SSITUs than for large organisations	X	
10005	SSITUs need less perceived cyber security vulnerability to support self-efficacy	C	10007, 11103, 11104, 11105
10006	SSITUs need to feel that their engagement in cyber security will result in a catastrophic breach ceasing to be inevitable	C	13307 + 11106
11106	Incidents impacting on reputation are likely to be catastrophic for SSITUs	X	

Table 12: *SSITU self-efficacy*

RID	Description	P	Conflicts
11108	SSITUs have inter-role conflicts of interest	X	12251
11116	SSITUs may be entirely virtual, without dedicated devices or services	X	12251
11124	SSITUs' security budgets are not high enough for suppliers to want to offer well-supported high-effort solutions	X	11111
11130	SSITUs are dependent on suppliers' quality of service	X	12251
11127	SSITUs lack a coherent/focused IT strategy, often using multiple solutions for the same activity	X	12251
11128	Supply chain requirements limit SSITU choices	X	12251
10008	Influential members of the supply chain need to increase the cost of SSITUs not engaging with security	C	10005, 10006, 11136

Table 13: *SSITUs' lack of influence*

RID	Description	P	Conflicts
12237	It is not possible to segregate users' multiple roles for best-practice access control	X	12251
11112	SSITUs may have no physical environment to secure	X	11132
11113	SSITUs are unlikely to have fixed networking infrastructure	X	11132
11114	SSITUs have high levels of home-working	X	11132
12234	SSITUs maintain a highly distributed IT system	X	11132
12235	SSITUs have a proportionately large attack surface	X	
13323	SSITUs have limited control of system layers	X	11132
13324	SSITUs lack the ability to employ multi-layered security models such as Defence-in-Depth	X	
12247	Standards assume SSITUs have a physical environment	X	11112, 11139
12248	Standards make tech-specific assumptions about the system to which they are being applied	X	11112–15, 11139, 12234 & 37, 13323
12251	The GDPR adopts the assumptions made by cyber security standards	X	11112–15, 11139, 12234 & 37, 13323

Table 14: *Multi-purpose system, system distribution and compliance constraints*

over the IT use they themselves need in their various roles (inter-role conflicts of interest — 11108), the various technologies and processes forced upon them by their supply chain (11128 and incoherent strategy — 11127), to the level of support and quality of service SPs are willing to offer SSITUs (11124, 11130).

This lack of influence is, in many cases, in conflict with 12251 — the GDPR's adoption of the assumptions made by cyber security standards. Not only do larger organisations have significantly different systems, they also have an unparalleled level of negotiating power, where SSITUs are 'price-takers' [129].

There is one final influence-themed requirement, voiced by some of the risk-holding stakeholders who have sought to influence the security of SSITUs — that they should be using their influence to make all SME suppliers implement cyber security, by punitively increasing the cost of accepting cyber security risk (10008). The framework records this requirement as being in conflict with the already catastrophic reputational risk faced by SSITUs (11106), the negative impact further risk would have on self-efficacy (10005, 10006) and SSITUs' inclination to accept non-reducible risks that would otherwise block their accepting contracts (11136). The requirement is unachievable because of a poor assumption made by the risk holder that their process of cost-benefit analysis is comparable to that of a SSITU — at the point where a catastrophic risk has failed to influence cyber security, a multiplication of that risk will have no positive outcome.

6.2.3.3 *Planning and application*

Unsurprisingly the multi-purpose system and system distribution constraints align with the system differentiators, to which they add additional detail — for example, the

artefacts that security measures are designed to protect (11139) include user credentials (12237), fixed networking infrastructure (11112) and a physical environment (11113). It is therefore also unsurprising that the detail that the constraints in Table 14 provide largely conflicts with 11132 (GDPR compliance).

Multi-purpose system constraints produce a number of requirements. SPs need to anticipate BYOD-style IT models (12207) and a multi-purpose IT system (12208) in their solution designs. They also need to protect the individual's right to freedom of internet use (likely to occur on work devices) to successfully secure very small organisations (12211) — as constraint 11108 suggests, the result of a multi-purpose system is the potential for conflicts of interest. Irrespective of whether the laptop belongs to the company or the solicitor, the directors in our scenario would be unwilling to purchase an additional device or duplicate software to allow them to segregate their roles: in micro companies directors often don't differentiate between company and personal expenses; rather, both will directly and noticeably reduce their personal income.

In anticipation of a distributed system, SSITUs need to protect their data irrespective of its location (13302), producing a fit criterion for SPs to implement security up to a GDPR-compliant level, irrespective of whether the data owner is an individual or an organisation. To actively participate in cyber security the SSITUs need to achieve optimum security at the endpoints (13312), which are likely to be the only system artefacts they control. However, SPs offering hardware are incentivised to force customers to purchase devices more frequently (11125) and SSITUs lack the money to invest in new hardware when the old devices are still functional but unsupported. SSITUs need to have longer-term updates in high-investment devices (smartphones, etc.) (13318).

The framework also highlights a number of GDPR compliance requirements, bounded by the technical constraints listed in Table 14 and building upon both ownership and context requirements. This leads to a set of GDPR-themed requirements that outline the processes that the GDPR expects, but with the addition of the following: SSITUs need to satisfy GDPR security requirements without having the prerequisite resources/infrastructure to comply with the standards those requirements are based on (13307); and SSITUs need to achieve the essence of cyber security standards without being able to comply with technical assumptions (11102). This leads to the following fit criteria: the suggested solution allows SSITU to afford comply with the GDPR without ceasing to operate and SSITUs can demonstrate compliance uniquely using the high-level goals outlined by standards (13307).

There are also a large number of planning and application requirements related to continuity, self-efficacy, digital footprint and system requirements derived from the preceding constraints. To retain the value and continuity of this discussion these requirements can be found in full in Appendix D.

The solution fit criteria for this set of requirements can be summarised as follows:

- anticipate a lack of user role segregation and that users cannot be tied to a specific location;
- recognise a strict budget and anticipate users prioritising endpoint security in this budget;
- facilitate GDPR compliance;

- hold all data (business and personal) with the level of security required by the GDPR; and
- don't block or slow any user activity.

6.2.3.4 *Adaptability*

SSITUs are IT-dependent (11135), and have legacy processes (13316) and extremely limited budgets, which do not typically stretch to specialist cyber security support (11118–23). While it may seem logical for solution designers to begin with the constraints and requirements describing problem ownership and business context, SSITUs are not developing a cyber security function from scratch (21111).

The framework therefore uses the 'adaptability' category to facilitate the capture of SSITUs' context-specific knowledge of the application of cyber security. Understanding these requirements, and the types of solution they have disregarded, allows the framework to transition from solutions that encourage SSITUs to take ownership of cyber security to encouraging SSITUs to take ownership of improving their cyber security to achieve an acceptable level of risk. This is a subtle but important difference.

Table 15 summarises the constraints and requirements related to adaptability, specifically in the context of evidence-based security.

SSITUs are constrained by the lack of resource and adaptability needed to support continual evolution (14402), resulting in a subset of SSITUs who need evidence before they will invest in the evolution of their cyber security practices — this is the group we named 'risk-evaluators' in Chapter 4.

Cyber risks are not any more catastrophic than other risks for SSITUs (12250) — *the difference is the unknown ability to reduce risk*, produced by a lack of evidence that their efforts are effective. This is demonstrated by SSITUs favouring availability and resilience in their choices (12246). They are not demonstrating a strong preference for high availability systems over privacy and confidentiality; rather, they are demonstrating a preference for security measures that provide a transparent return on investment, which can be compared with other expenditures.

SSITUs then also favour measures with a transparent cost (12238) — it is for this reason that SMEs state a preference for technical solutions. For alternative types of solution to become more acceptable SSITUs have to be able to enumerate their cost (including the burden of configuration and use) (12206, 12227).

These constraints, combined with the requirement for adaptability in a changing environment, have resulted in the following requirements: the need for evidence-based solutions (12226); for impactful solutions to become cheap and easy to adopt (12215); and for high-quality outsourced services to be affordable (14401).

These requirements produce some interesting fit criteria, linking these category 5 requirements to contextual and planning requirements to complete the cyber security lifecycle. Namely, that solutions are fully costed, are offered with user-friendly evidence of their effectiveness that facilitates solution comparisons and can be implemented by novices.

RID	Description	P	Conflicts
14402	SSITUs are constrained by the lack of resource and adaptability needed to support continual evolution	X	11132
11118–23	Budgetary constraints	X	
12250	Cyber risks are not any more catastrophic than other risks for SSITUs	X	11142, 11132
12246	SSITUs favouring availability over confidentiality and resilience over pro-active security in decisions	X	
12238	SSITUs favour security that has a transparent cost	X	12208, 11124, 11125
12206	SPs need to enumerate the burden of security measures' configuration and use and include this in their evaluation of acceptable price	C	11104
12227	SSITUs need non-technical solutions to be enumerable/-comparable against technical measures	C	11104
12226	SSITUs need evidence-based solutions	C	11104
12215	Solutions need to make impactful security decisions easy to adopt	C	11136
14401	SSITUs need high-quality outsourced services to achieve adaptability in a sustainable way	C	11124, 11129

Table 15: *Evidence-based security*

6.2.4 *Evaluation*

The requirements set presented in this section is abstract, the framework scope having intentionally excluded solution-specific requirements in favour of the reusable global constraints and requirements SPs need to design for this sector. However, it is possible to assess the validity of the framework, within the bounds of its scope, against the requirement validation process described in Chapter 3.

6.2.4.1 *Individual requirements*

Individual requirements have to be validated based on their scope, relevance, completeness, ambiguity, consistent terminology, viability within constraints and to ensure they are not solution-bound.

The majority of requirements fit these criteria within the scope we expected to achieve in this generalised framework. Their completeness and relevancy will depend on the solution each framework user is intending to implement. For example, a high level understanding of the system architecture provided in our scenario might be useful to someone developing advice for micro-SMEs, whereas application requirements relating to those system attributes might be irrelevant. In contrast users developing technical solutions will have a large number of functional requirements to develop, as well as a number of additional non-functional requirements to elicit, depending on the other SP stakeholders relevant to that system attribute. Section 6.2.4.2 provides further information about requirements SSITUs are expecting their ecosystem to dictate.

There are also a number of constraints without a fit criterion. In this case the constraint is likely to have contributed to multiple requirements, which have their own fit criteria.

The biggest exception, in terms of relevancy, is requirement 10008 — that influential members of the supply chain need to increase the cost of SSITUs not engaging with security. This requirement is sourced from the RH stakeholders, placing it outside of the scope described in Section 6.2.1. It was not included in the requirements framework with the intention that solution developers attempt to implement it: as discussed in Section 6.2.3 it is impossible to implement within the SSITU context, and it should be discarded at this quality gateway.

However, requirement 10008 has served its purpose — to highlight in this structured context why some expert dialogue and expectations of SSITU business risk management systems are harmful to SSITUs' adoption of cyber security.

Some requirements, for example those related to evidence-based security, meet the criteria of being viable *within the system constraints.* However, subjects such as the development of usable and relevant metrics for decision making are cyber security grand challenges. A requirement's existence and the use of metrics being feasible within a SSITU's system does not reduce the challenge presented by Pfleeger and Cunningham of proving a negative [81].

The viability of any GDPR-related requirements within the specification constraints is questionable. This is discussed in more detail in Section 6.2.4.2.

6.2.4.2 *Specification completeness*

Chapter 3 presented the measure of completeness of a requirements specification using two criteria:

1. Each expected requirement type (Table 4) is represented in the specification.
2. The use cases have been identified and subsequently satisfied.

Criterion 1 comes close to being satisfied, with the exception of two requirement types: robustness and fault tolerance (R/F) requirements; and maintenance and supportability (M/S) requirements. Other requirements present in the framework provide an explanation why SSITU participants did not provide sufficient information to record their requirements for cyber security solutions' robustness, fault tolerance and maintenance and supportability.

There are several global requirements and constraints relating to ownership, self-efficacy and adaptability that describe how SSITUs limit themselves to technical solutions that avoid any maintenance requirement in order to fix and control cyber security costs. They also describe how SSITUs expect solution support and a distribution of responsibility with their SPs as a usability requirement, and how SPs constrain their access to that support. However, these requirements were described in the context of planning an organisation's cyber security.

The over-arching constraints that SSITUs have no influence over contract terms and have very little control of their systems highlight a SSITU's expectations when describing requirements. These constraints are placed on the underlying technical systems as well as any cyber security solution the SSITU attempts to apply to them, meaning that they are not considered solution-bound and are fully within scope. But these

constraints on influencing and accessing the underlying system have pushed two non-functional requirement types (R/F and M/S) into a solution-specific scope — SSITUs are consumers supplied with technological 'black boxes', resulting in some requirement types being delegated to the SPs to define.

While all other types of requirement are represented in the framework, there are likely to be subsets of other requirement types, for example precision, accuracy, and extensibility, which have been excluded by SSITUs with the expectation that they are solution-specific and controlled by SPs.

For criterion 2, solution-specific use cases are out of scope; however, with GDPR compliance as a high-priority requirement there are two use cases to evaluate against: that scoped by the context diagram (Figure 40 — to add security to the fully-controlled parts of the SSITU's system); and the expectation of best practices presented by the GDPR.

The work described in the context diagram is fully satisfied. Although giving a structured presentation of the constraints surrounding this cyber security goal, the goal in itself is not a novel problem. The aggregation of these constraints illustrates why SSITUs might focus on optimising endpoint security and scopes cyber security to match their perceived self-efficacy — a scope, it should be noted, that is generally far narrower than that of even Cyber Essentials [111].

The priority given to reputational risk reduction and compliance was a surprising outcome of this framework and in many ways conflicts with the scope described by the essential business case. This is because the need to comply with the GDPR, the assumptions it makes and the specific technical requirements it raises, conflict directly with the constraints this framework was intended to present.

The extent to which constraints derived from legislation conflict with the system SSITUs' business context and SPs (and to some extent RHs) allow SSITUs to implement provides more in explanation of why SSITUs struggle to maintain their cyber security self-efficacy, than in offering suggestions how SSITUs might be assisted in aligning themselves with the GDPR.

What it does make clear is that the stereotypical micro-SME is not going to be able to comply with the security requirements of the GDPR where it adopts the assumptions of cyber security standards. As discussed in Chapter 2, the scope of cyber security requirements in the GDPR go well beyond the implementation of Cyber Essentials. This means that, even with the GDPR's provision that 'reasonable' levels of security might be demonstrated through compliance with the appropriate standards, the requirement for accountable decision making on behalf of data subjects leaves SSITUs already engaged with cyber security open to penalties.

Due to their status as organisations rather than individuals, a large proportion of SSITUs become consumers whose cyber security risks are increased rather than mitigated by the stipulations of data protection legislation.

To comply with the GDPR, SSITUs need to be able to engage with all five categories of cyber security principles. Referring back to Figure 38 (a technology and business process agnostic description of cyber security best practices), Figure 43 provides a summary of the requirements framework, highlighting the barriers it describes that limit engagement with best practice, some of which can be circumvented by the introduction of additional requirements and some of which (labelled a–e) constrain SSITU cyber se-

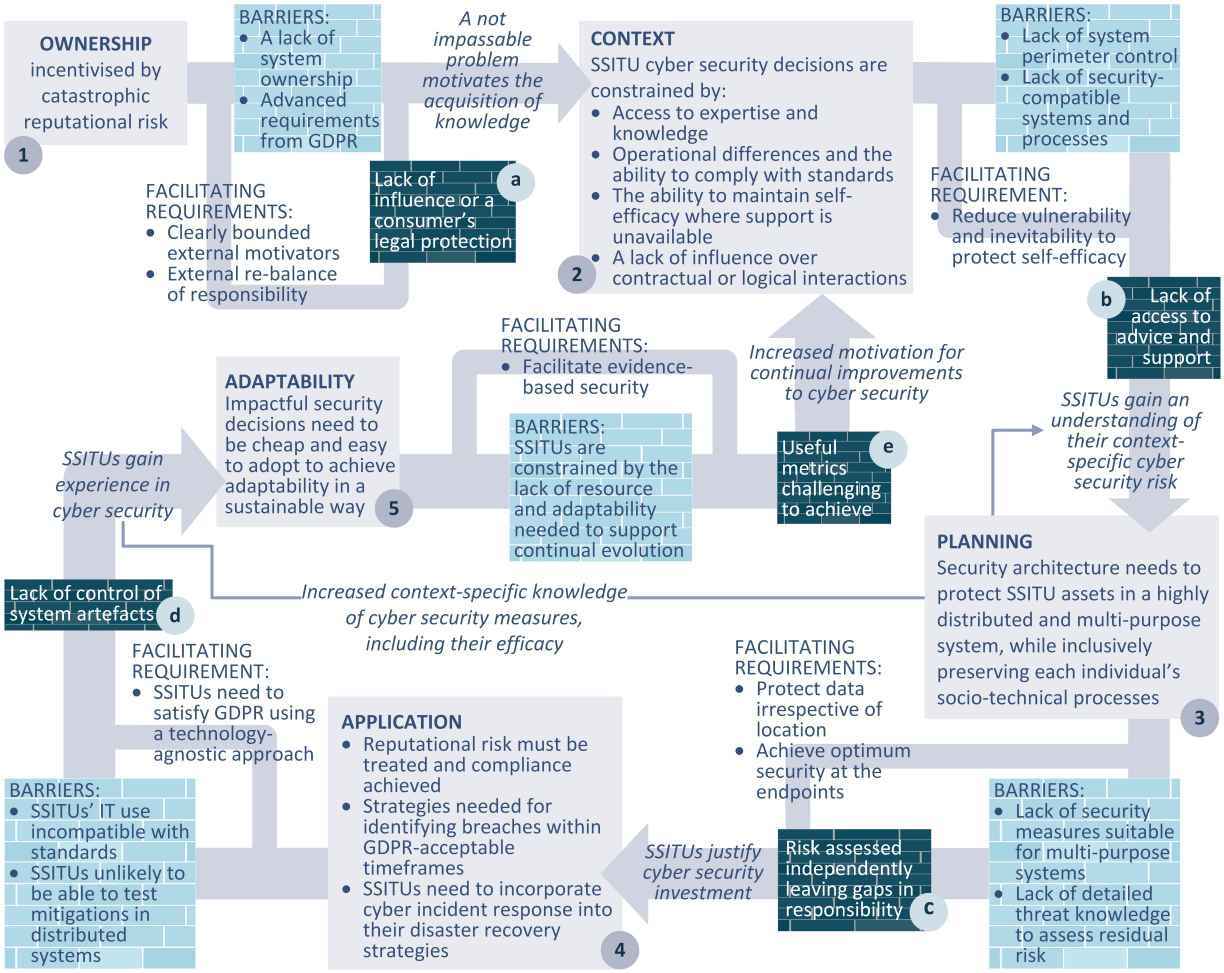


Figure 43: *SSITU cyber security requirements framework summary*

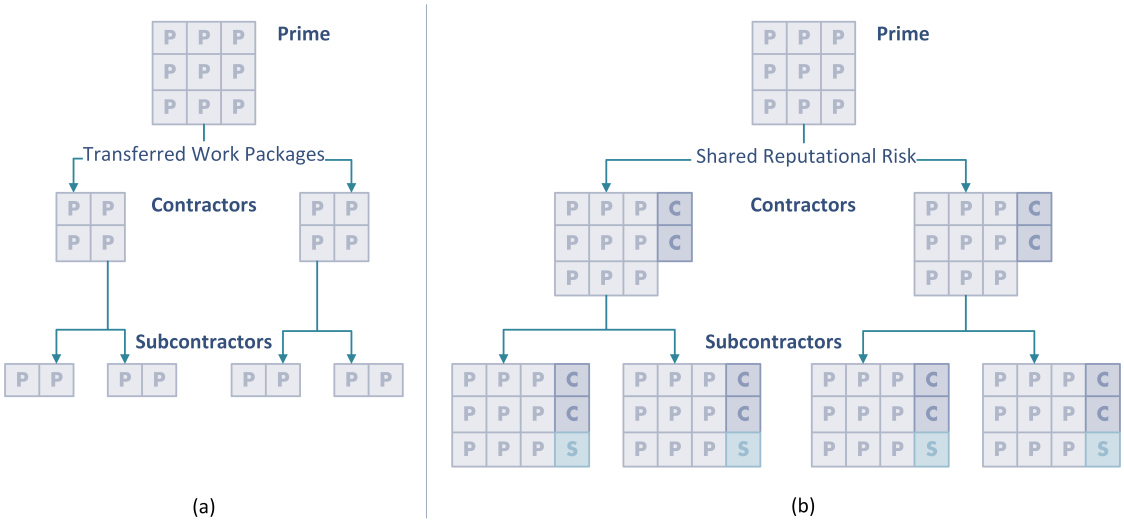


Figure 44: *Transferred project work packages versus shared cyber security reputational risk*

curity decisions to the point that achieving even a technology-agnostic comprehensive implementation of best practices becomes impossible.

Labels a-e denote barriers that can only be addressed by the wider supply chain. This strengthens the argument for developing the cyber security requirements framework for supply chain risk holders. The role *influence* plays in the barriers SSITUs face means that, although this analysis describes a scenario where SSITUs might be incentivised to engage with best practices, they would not be in a position to sponsor a supply chain scoped requirements specification. However, the requirements described in this framework should act as reassurance to RHs engaging with supply chain security problems that SSITUs have some incentive to evolve their systems.

6.3 A CYBER SECURITY REQUIREMENTS FRAMEWORK FOR SUPPLY CHAIN RISK HOLDERS

The cyber security requirements framework for supply chain risk holders (SCRHs) described in this section follows the same structure as the framework for SSITUs provided in Section 6.2.

6.3.1 *Stakeholders and their goals*

The three stakeholder groups contribute to this framework, but, in contrast to the framework described in Section 6.2, this framework uses the common scenario of a large RH as the project owner, contracting a SP (who is likely to be another large organisation) to develop a solution (20001), addressing problem 2 from Section 6.1 (21109). The solution is intended to be implemented by SSITUs, or across the supply chain, but the customer is undetermined (20002).

The requirements are provided by SCRHs, with SSITUs contributing constraints. The goal is to reduce the cyber security risk to RHs' assets, whose value is orders of magnitude greater than the total assets held by an SSITU, but where the SSITU plays a key role in securing the RH's assets.

6.3.2 *Essential business case*

6.3.2.1 *Context diagram and framework scope*

The solution may be intended to be implemented by SSITUs, or across the supply chain, but the customer is undetermined. Summarising the findings of Chapters 4 and 5, SSITUs are typically treated as consumers or 'price-takers' by their supply chains — as Figure 36 illustrated, SSITUs are constrained from all directions in the supply chain by their small budgets and lack of influence.

Therefore, the most pertinent question this requirements framework needs to address is *who is the main investor?* As illustrated by requirement 10008 in Section 6.2, SCRHs using their influence to attempt to force SSITUs to treat the risk transferred to them have instead found their risks accepted. Section 6.2 also presented the constraints that will define the capacity SSITUs will have to reduce supply chain risk. Until a business case is made for a named stakeholder (with the capacity to act) to be the investor for supply chain cyber security, supply chain risk will not be reduced.

This aligns with issues in the field of safety, described by [53] and discussed in Chapter 5 — that a complex supply chain introduces gaps in responsibility, where safety hazards (or in our case cyber security risks) are far more likely to occur.

The survey presented in Chapters 4 and 5 unearthed both the security disincentives for organisations in interdependent systems described by van Eeten and Bauer [119]: a vulnerability of SSITUs facing a threshold for optimal investment so high that they opt for resilience over security, and "negative network externalities". Our participants are describing a supply chain scenario which is known to dissuade certain stakeholders from investing in cyber security.

As illustrated by Figure 44(a), projects traditionally transfer small work packages to contractors and subcontractors. This risk is often accepted, rather than reduced, by SSITU subcontractors. Because the overall risk of a small contractor failing will have limited impact on the project, and small contractors are cost-effective, the project owner accepts that SSITUs operate at a higher risk.

Unfortunately, the supply chain is approaching the cyber security risks associated with their interactions in a similar manner — large RHs are transferring cyber security risk to the SSITUs who interact with them, without realising that reputational risk is both indivisible and non-transferable. As Figure 44(b) illustrates, RHs are sharing rather than transferring their risk throughout the supply chain. Their reaction to this has made an enormous contribution to the small-scale cyber security dialogue, as they attempt to use their influence to force SSITUs to implement sufficient security to mitigate against the risks they transfer, but without providing them the business case to achieve change. SSITUs in this supply chain scenario have a high level of influence over the *cyber security* of other organisations, but are not being treated as *influence-holders*.

In addition to this, according to van Eeten and Bauer, the difference in capability across the supply chain acts as a disincentive in itself [119]: the more the large RH invests in security, the more they differentiate their security from that of their small suppliers, and the more appealing those SSITUs become as targets. Reinforcing inequalities in the supply chain may be reducing SSITUs' self-efficacy.

The framework needs to produce requirements under which SSITUs might be able to participate in securing the supply chain, with the eventual customer being the RH, the SSITU or the wider supply chain as an ecosystem of partnerships.

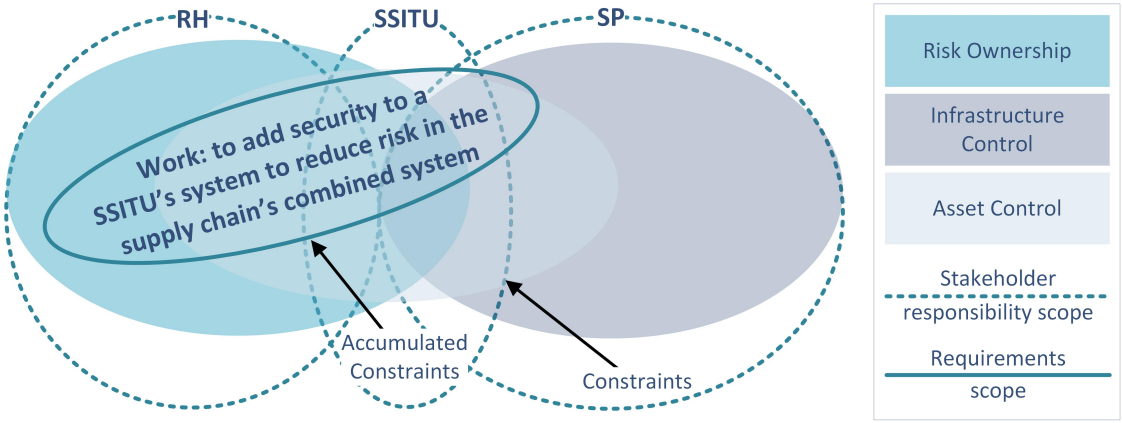


Figure 45: *Context diagram for the requirements framework for SCRHs*

Figure 45 provides the context diagram for this requirements scope. As can be seen, in contrast to Figure 40, there is no overlap in responsibility scope between the RH and the SP. As characterised by the term 'supply *chain*' each organisation in the chain acts as an intermediary for the next. In technical terms, this means that the constraints described in this framework are accumulated across a series of interactions; in legal terms (as discussed in Chapter 5) the degree of separation diminishes responsibility for mitigating risks.

The requirements scope encompasses a large portion of the SSITU's system, which is to be secured. However, it also contains a non-trivial amount of the risks owned and assets controlled by the RH. This is intended to encompass the interfaces between adjacent systems and to illustrate that the aim of this framework is to secure the RHs' assets irrespective of their location. There is also a small overlap with the infrastructure controlled by the SP. This is because, to influence the SSITU's security, the RH may need to influence the SP.

In short, the scope of this framework means that it will emphasise the large RH using its influence to decrease the level of security inequality of the SSITUs in its supply chain, whether by investing in direct risk mitigation or by influencing the security benchmark for services within the price range of the SSITU. It works with the key assumption that the RHs are aware that risk transferred to SSITUs is likely to be accepted without mitigation, and that RHs understand why enforcement without investment is not likely to produce the desired effect. It also assumes that the supply chain needs to facilitate the continued presence of SSITUs, for reasons of both cost and to provide access to specialist knowledge, making the business case for additional security investment from the RH/large SPs.

6.3.2.2 *Sample scenario*

The scenario uses the example of a large medical organisation, which has been provided access to a sample of pseudonymised patient data by the National Health Service (NHS). The data is to be used to facilitate research into prescribing practices across an extremely distributed organisation.

The scenario company mainly employs medical experts, so has outsourced the development of data-mining algorithms to a SSITU that specialises in artificial intelligence.

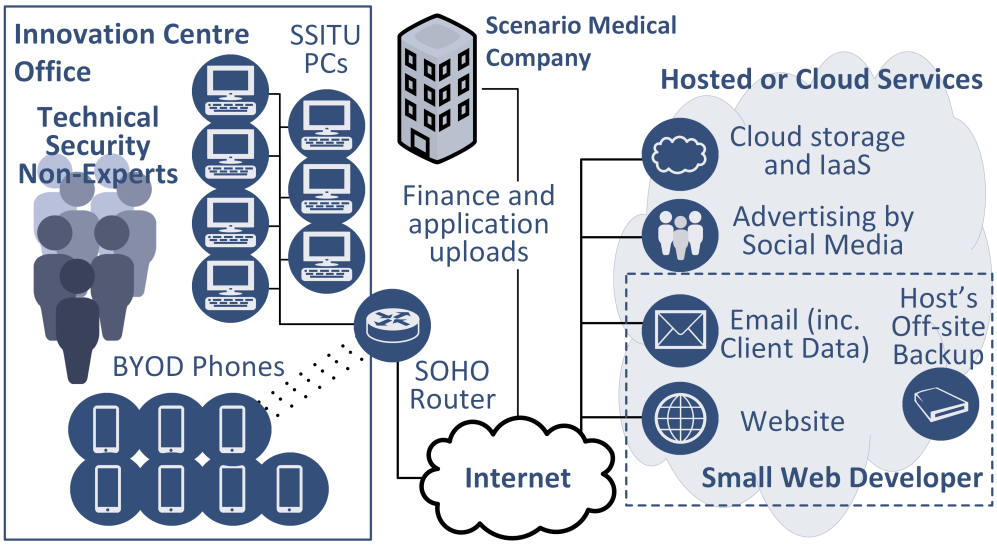


Figure 46: *SCRH framework scenario architecture*

In order to train their algorithms the SSITU needs access to a large portion of the customer's dataset, so have been provided with 1 million records. Owing to the size of the SSITU, the size of the dataset and the processing power required to run their algorithms, the SSITU has arranged for the sample data and codebase to be hosted by a large cloud infrastructure provider, under their standard terms of service.

The SSITU has only 7 employees, all based in the same office. Although they are a technology company they are not yet big enough for them to have dedicated IT function. The proportion of knowledgeable employees makes it harder for the company directors to stop them circumventing security measures, but the employees are coders, not security specialists. Thanks to their use of Infrastructure as a Service (IaaS) they have also limited their infrastructure requirements to the point that they are still able to function using the routing and services provided in the innovation centre.

Like the scenario in Section 6.2 this SSITU also has a website configured and hosted by a small web developer, an email server and various social media accounts.

SSITU employees only use company devices to access the sample data, but are in the habit of exchanging ideas and asking colleagues advice via WhatsApp on their personal smartphones. In addition to the responsibility the SSITU has for the data they hold, they also maintain two logical links into their customer system. The first is an application interface that allows them to deliver algorithms to their customer's researchers to apply to the full dataset. The second is a set of login credentials for the customer's billing platform, which allows them to raise invoices for the work they complete.

There are clear differences between this and the scenario provided in Section 6.2. Both scenarios relate to a micro-SME, but this scenario has a far clearer logical link to a large customer, as well as having even fewer system artefacts fully controlled by the SSITU. A network diagram illustrating the environment is given in Figure 46.

RID	Description	P	Conflicts
21117	RHs need cost-effective or niche (and so often smaller) suppliers	X	21116
21110	Supply chain security models need to accommodate the selection of small suppliers for contracts	C	11121 + 20005
21114	Contracts need to be satisfied across the supply chain	C	20007, 21116
21112	RHs need interconnected systems for efficiency	C	21116
21113	Stakeholders need interlinked services to increase reliability for their customers	C	21116
20008	RHs need to have a better understanding of consequences and limitations of outsourcing when developing contracts	C	11129, 11131
20003	Stakeholders need clearer responsibility/ system transparency within the supply chain	C	
20005	RHs need to secure the supply chain to secure their larger organisations	C	21116
21116	Degrees of separation between between risk-holding and risk-influencing stakeholders, as well as contractual limitations, limit the ability to transfer responsibility with risk	X	
21118	SSITUs can't afford to lose customers by disclosing breaches in order to ask for support, delaying RHs' incident response	X	21114, 11132

Table 16: *Inter-organisational processes and the division of responsibility or risk*

6.3.3 *Requirements*

The framework for SCRHs supplies requirements in five themes that augment the framework described in Section 6.2, adapting it for the wider supply chain:

- Ownership and context
  - Inter-organisational processes
  - The division of responsibility
  - Supply chain risk reduction as an incentive
  - Protecting SSITU self-efficacy
- Planning and application
  - Shared influence
  - (Requirements derived from the preceding constraints)

6.3.3.1 *Ownership and context*

Constraints and requirements themed around inter-organisational processes and the division of responsibility or risk are summarised in Table 16. The first constraint begins by highlighting how important smaller organisations are in providing cost-effective or niche services to large organisations (21117). Cyber security is, in many cases, inconsequential when SCRH choose their suppliers — before 2013 [84] it wouldn't have

occurred to a SCRH to audit their *heating and ventilation* contractors for cyber security. In the same way that SSITUs will accept risks where mitigation would disrupt business processes, the supply chain is accepting risks to avoid having to limit the number of SSITUs they interact with.

For reasons of efficiency and reliability the supply chain needs to continue (and potentially increase) their use of interconnected systems (21112, 21113) and secure these processes (20005), but this conflicts with the need to accommodate the selection of small suppliers who have a limited capacity for security (21110). As a result there are a number of requirements related to how responsibility and risk is considered to facilitate these interconnections (21114, 20008, 20003).

There are constraints that limit the adaptation of contracts across the supply chain, most notably that the attack vector may not come from a directly adjacent system (21116). In this case the degrees of separation between source and victim reduce the liability of the organisation attackers used to reach their target (although it would not necessarily reduce the reputational damage to that organisation).

Requirement 20007 states that contracts need to be satisfied across the supply chain, however, this conflicts both with the self-efficacy requirements discussed later in this section and with 21116, as SCRHs find it challenging to transfer responsibility and accountability across the supply chain, making it difficult for them to enforce their contracts.

If the scenario medical organisation wanted to audit the quality of cyber security offered by the SSITU developer, they are dependent on the SSITU having sufficient influence to extract that information from their large cloud supplier. Although, given the sensitivity of the data they control, it would have formed part of due diligence to verify the security the service offered at the point of purchase, they may experience time-consuming difficulties in verifying this information during the course of the contract. The terms of service may seem vague, publicly available information about security measures and processes may be limited, the supplier may not feel obligated to provide detailed information, and the service is likely to be offered under fixed terms to control the SP's costs.

There is also a constraint around transparency. SSITUs, whether employees, contractors or suppliers, equate reporting cyber security breaches with the consequences of reporting failures in any other function of their role. This situation cannot be improved by the victim-blaming culture that has evolved in cyber security, where incidents are reported to have occurred because the victim foolishly ignored their SP's advice[4].

SCRHs may be delayed responding to incidents because, if they are able to avoid it, SSITUs will not disclose security breaches (21118). This may conflict with compliance requirements in both business-to-business contracts (21114) and for the GDPR (11132). However, if the reputational damage of disclosing a breach would be catastrophic for the SSITU, they have got nothing to lose by failing to implement the measures that would allow them to detect an incident.

One participant described how employees had been too 'embarrassed' to report mistakes, increasing his burden (as IT Director) to monitor the systems. One may ask, to what extent do we incentivise SSITUs to hide their mistakes?

4 "NHS WannaCrypt postmortem: Outbreak blamed on lack of accountability. Plus systemic underspending in IT." — www.theregister.co.uk/2017/06/29/nhs_wannacry_report/

Due to the financial constraints faced by SSITUs highlighted in our previous discussion, protecting SSITUs' self-efficacy becomes as relevant to securing the supply chain as it was to developing solutions uniquely for SSITUs. The supply chain needs to support and encourage SSITUs' autonomy. Although this largely relates the use of SCRHs' influence in the planning and application of supply chain security, there are two requirements, sourced from SSITUs and summarised in Table 17, that relate to context and problem ownership in this framework.

The first is the avoidance of placing unmitigable levels of risk onto SSITUs (20007), for the same reasons mentioned in Section 6.2. Once SSITUs have been given achievable goals, the second requirement is for the supply chain not to assume that they have *no security* because what they are doing is not comparable to the best practices in larger organisations (21111). When our scenario organisation has invested in cyber security within their constraints, an auditor measuring their efficacy as 'nil' can only dissuade them from further engagement with cyber security.

The accumulated fit criteria for this set of requirements, when considered alongside the SSITU framework that this framework extends, can be summarised as follows:

- The solution allows IT systems to be interconnected.
- Organisations' responsibilities are clearly defined.
- Responsibilities are defined with a reasonable expectation of what SSITUs can achieve.
- SSITUs are expected to achieve a benchmark level of security — they are expected to take ownership of their cyber security risk in line with 11101.
- Contracts focus on reducing rather than transferring risk.
- A solution is: a default setting; can be achieved and maintained by novices; or it becomes one of the security measures *SSITUs* consider a benchmark requirement for reasonable cyber security.
- Solutions are usable by individuals in a home environment and do not suggest that SSITUs cease to carry out any activity.
- SSITUs' own security and privacy processes are preserved.
- The solution is presented to the SSITU in a way that makes them certain that it will have a measured effect and they can easily implement it.
- There is a combination of solutions that allow SSITUs to comply with the most reputationally damaging of: the GDPR; or customers' cyber security expectations.

6.3.3.2 *Planning and application*

Although the constraints and requirements relating to ownership and context have generated additional planning and application requirements, there are also influence-themed requirements that fall into the planning and application categories of best practice.

RID	Description	P	Conflicts
20007	SSITUs need influential members of the supply chain to cease to transfer unmitigable levels of risk to them	C	22210
21111	SSITUs need larger stakeholders not to assume that lack of standards compliance/ equivalent practices means no security	C	12248, 11117

Table 17: *Protecting SSITU self-efficacy*

With the exception of 20006, these requirements, summarised in Table 18, are not aimed at SCRHs attempting to influence SSITUs' own implementation of security. The rationale for 20006 is that, while forcing SSITUs to reduce SCRHs' risk has been unsuccessful, influencing the benchmark of 'basic' security expected of SSITUs and enforcing that is felt to be feasible. This requirement aims to ensure that SSITUs are taking responsibility for their cyber security within the scope described by the requirements framework for SSITUs.

The other requirements are intended to use the influence SCRHs hold, not to push additional risk and requirements onto SSITUs, but to encourage the changes SSITUs need but cannot prompt suppliers to make (22212, 22213).

This approach is not entirely unfamiliar, with the US Government attempting to use their influence to shame suppliers into increasing the quality of their cyber security[5]. The difference is that, where governments have to avoid showing bias towards specific SPs, large commercial SCRHs have the capacity to build partnerships with SPs. Although this does not change SSITUs' budgets, and without careful negotiation will conflict with the issue of specialist security-accredited services being outside of the price range of SSITUs, it may provide them with a more (transparently) secure option than they could otherwise have accessed. This contrasts with the example given in Section 6.3.3.1 of the quality of cloud security our scenario SSITU might currently experience.

One advantage of a partnership within the supply chain is that, where governments lack the resources to support small organisations on a large scale, they do interact with large risk holders. The aggregation of risks across the supply chain should assist that supply chain in interacting with the government as it chooses how to deal with the international nature of cyber security threats (22205).

There is also scope for the supply chain to develop a lobbying function, and while SCRHs (who have the capacity to contribute to standards, etc.) may wish to represent SSITUs' interests in those workshops (22212), they can also use the scale of their risk to lobby for better consumer protection (11129).

If the scenario SSITU (or one of the medical company's home-working employees) used a SP who had sustained multiple breaches by opportunistic and low-skilled attackers, the large medical provider would probably prefer that that SP's relationship to an adjacent system be terminated. In the TalkTalk scenario described in Chapter 5, the SP was able to convince SSITUs that the burden (and potentially risk, if the SP did not accept their lack of "reasonable care and skill" [113] and pursued them for non-payment) of attempting to terminate a contract early was greater than the security

5 US government probes mobile phone industry over the sad state of security updates: arstechnica.co.uk/security/2016/05/ftc-fcc-mobile-phone-security-updates

RID	Description	P	Conflicts
20006	Influential members of the supply chain need to increase the cost of SSITUs not engaging with basic security	C	
22212	SSITUs need large risk holders to influence large suppliers on their behalf	C	11124
22213	The supply chain needs to reduce the incentive for large organisations to retain/grow their control over consumer systems	C	11129
22205	The supply chain needs to mitigate against the international nature of threats	C	11105
23312	The supply chain needs suppliers to allow SSITUs to terminate contracts when persistently poor cyber security practices are demonstrated	C	11129

Table 18: *Shared influence*

risk they posed. In reality the cost of proving breach of contract in this case may have been greater than the cost of paying to leave the contract, but SSITUs run on tight margins and depending on which service is affected may not be able to afford to extricate themselves from low-quality services.

The solution fit criteria for the categories of planning and application, again amalgamated with criteria from the SSITU framework, can be summarised as follows:

- communicate cyber security responsibilities and requirements using a consistent common vocabulary;
- provide clear contractual responsibilities;
- large RHs influence SPs to increase the quality of solutions available;
- security should be approached as a partnership, with communication and support offered where required;
- SSITUs can obtain information from their SPs to satisfy GDPR accountability requirements or an equivalent customer audit;
- anticipate a lack of user role segregation and that users cannot be tied to a specific location;
- recognise a strict budget and anticipate users prioritising endpoint security in this budget;
- facilitate GDPR compliance;
- hold all data (business and personal) with the level of security required by the GDPR; and
- don't block or slow any user activity.

Requirements and criteria for adaptability are carried forward from the SSITU requirements framework and can be found in Section 6.2.3.4.

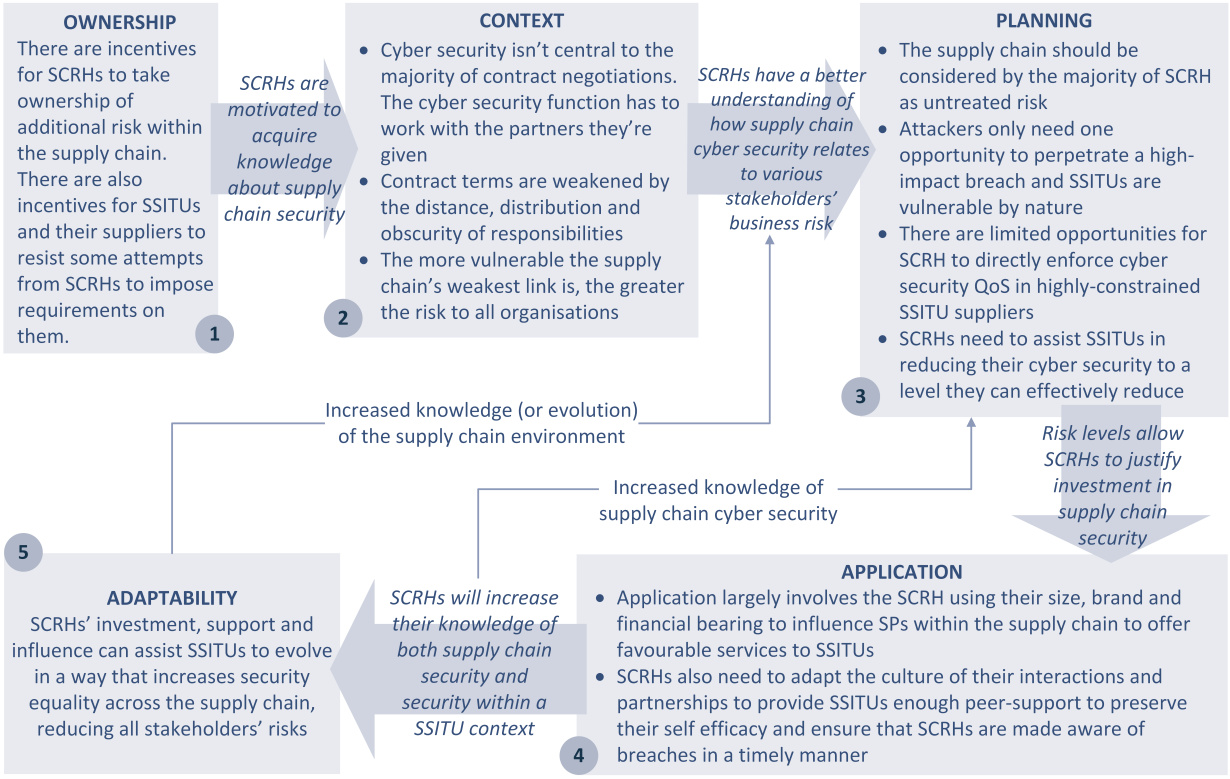


Figure 47: *Supply chain RHs' cyber security requirements framework summary*

6.3.4 *Evaluation*

In terms of validity, the individual requirements are of an equivalent quality to those presented in Section 6.2. As the framework is an expansion of the SSITU cyber security requirements framework it has the same strengths and weaknesses — requirements will be of varying relevance depending on the specific solution and any user will need to develop functional requirements. There are also some requirements, related to standards, etc., that are on a time-scale which may not be compatible with a specific project. These requirements are more relevant to large SCRHs with mature cyber security functions to consider over multiple iterations of the five categories of cyber security principles.

Due to the complexity of supply chains there may be some themes that were not discernible by the present author — we expect the number of non-functional requirements to expand when placed into a specific supply chain or business sector context.

Once again referring to Figure 38, Figure 47 provides a summary of the requirements framework, framed by the high-level processes of cyber security best practices.

The way that the framework contributes to each category of cyber security principle indicates both: that it should be feasible to make the business case for SCRHs to invest in securing their supply chains; and that this framework manages to take into account the constraints of SSITUs and the common understanding of cyber security best practices held by SPs and RHs.

In comparing the two frameworks it is possible to identify a duality of purpose in the SCRHs' framework: barriers a–d, described in Figure 43, are tackled directly by the framework as reducing these barriers also reduces supply chain risk. Barrier e is

not explicitly handled, however, the framework makes the case for SCRHs to invest in encouraging self-efficacy in SSITU cyber security — a goal the SSITU framework suggests is related to increased levels of evidence-based security.

In some supply chains, risk from poorly secured SSITUs could incentivise SCRHs to invest in a way that also allows those SSITUs to resolve their security issues. This scenario is likely to relate to a specific subset of SSITUs — suppliers who focus on retaining a small number of large high-value clients. Other SSITUs will be harder to reach and influence, but the changes SCRHs need to influence SPs to make could have further-reaching consequences, benefiting the SSITUs outside of these supply chains.

6.4 SUMMARY

In this chapter we have evaluated how the context that SSITUs operate in fails to provide the foundation for implementing current cyber security best practices. The framework and scope suggested in Section 6.2 would produce cyber security measures that are achievable for the majority of SSITUs — measures complementary to those suggested in Cyber Essentials [111], for example. However, offering additional security to the broader supply chain is more challenging. The framework offered in Section 6.3 offers some insight for organisations attempting to reduce their own risk or develop a product for this sector.

These requirements frameworks have an influence on the applicability of the building blocks of cyber security 'best practices' as they are currently perceived. However, as our mapping of our evaluations to Figure 38 illustrates, they still align with the essence of the problem cyber security best practices are attempting to solve. Some problems do need to be tacked at a supply chain level for the inequalities between small and large organisations in the supply chain to be redressed. Taking the outcomes of our previous survey and re-framing its outcomes as requirements has not only provided us with the framework we intended to create, it has elicited or prioritised a number of themes that contribute to our understanding of the small-scale cyber security ecosystem.

The frameworks have been validated within the criteria offered to us by [90] — namely that we have tested the requirements frameworks for individual accuracy and specification completeness. As the knowledge we elicited these requirements from was the result of a previously peer-reviewed UK case study we do not anticipate any dramatic changes to the essence of the work should this be applied by projects operating within the UK. We would, however, expect for there to be a need to revise the wording of some requirements as they are adopted, in addition to projects facing the issues described in our framework evaluations — that producing a solution that fits some stated requirements is challenging. Only time and use will fully evaluate the usability of our frameworks.

We would expect that these frameworks would adapt to any EU state, given that the only 'best practice' that is specific to the UK is Cyber Essentials and the fact that there is a small number of cultural differences in the IT use of SSITUs in the various EU member states. Other regions would have to make significant changes. For example, the USA has significantly different data protection requirements (largely taking a sectoral approach), which, owing to SSITUs' concerns over reputational damage, could significantly change requirements. In contrast, African states have a significantly different network infrastructure, with the majority of internet users relying on mobile data

connections, which pass via satellite connections — the differences in the devices used and the bandwidth available may also prompt the adaptation of these requirements. Chapter 7 reflects on these frameworks and the contributions made by this dissertation.

7

CONCLUSIONS

This chapter reflects on the contributions, limitations and future direction of the research presented.

Section 7.1 refers back to the research questions outlined in Chapter 1, relating them to research outcomes and reflecting on their contribution. Section 7.2 discusses the limitations of this research and Section 7.3 outlines the direction any future research grounded in our contributions may take.

7.1 CONTRIBUTIONS

In Chapter 1 we introduced our research by asking *"if existing large corporate cyber security and governance practices are not well adapted for small organisations, how might we enumerate and articulate small-scale IT user requirements for security?"* This question was informed by the introduction of four research questions.

We began our evaluation of these research questions in Chapter 2, where, informed by an initial study [76], a comprehensive literature survey and the presentation of our project scope and aims [71], we responded to the question *"who are the members of the small-scale cyber security ecosystem?"* (research question 1) and described current practices relating to the security of this user group.

In Chapter 4 we responded to research question 2 — *"how do the constraints of a small organisation influence their risk perception and how they justify security investment?"* by providing a better understanding of the realities of SSITUs' business operating environments and, consequently, how they approach cyber security risk and decision-making [75].

This was followed with a description of the way SSITUs use technology and the constraints this places on their adoption of cyber security best practices [73] (Chapter 5) — a response to *"once a SSITU has justified investing in cyber security, what constraints within their IT system limit their decisions?"* (research question 3).

Collectively the contributions of Chapters 2–5 gave the background information needed to *enumerate* SSITUs' cyber security requirements. Using the approach described in Chapter 3, Chapter 6 *articulates* these requirements [74]. We provided two requirements frameworks for the small-scale cyber security ecosystem, responding to research question 4: *"how can understanding the context that SSITUs operate within assist in the development of a small-scale cyber security requirements framework?"* The chapter also discussed how these requirements relate to the best practices presented in Chapter 2; highlighted discrepancies between SSITU capabilities and those best practices; and discussed how the gap in expectations between SSITUs and RHs might be addressed, or the cyber security inequality between SSITUs and their supply chain reduced.

To a certain extent the contributions of this dissertation change depending on the perspective of the audience and the way the information is framed. Sections 7.1.1–7.1.4 discuss the impact this research may have on four stakeholder groups — the stakeholders outlined in Chapter 2 and academia.

7.1.1 *Contributions to SSITUs*

The aim of any organisation's cyber security function, as described by Pfleeger and Pfleeger, is to develop a *'reasonable'* level of security [80] — an expectation of perfect security being both unreasonable and impossible. They use four key principles to assess whether reasonable security has been achieved: that the organisation expects attackers to use any available means of access; knows security won't be stronger than its weakest link; selects security measures to proportionately protect assets given their value; and selects effective controls, which must be efficient, easy to use and appropriate.

Pfleeger and Pfleeger's principles highlight perfectly the motivation for carrying out this study. From the outset, with the completion of our initial study [76], it was obvious that the small-scale cyber security problem was one of articulating what 'reasonable' cyber security represented for SSITUs, in the face of both pressure and poor assumptions from the RH and SP stakeholder groups.

For SSITUs, with their characteristically low-knowledge, lack of resource and limited influence, simply identifying achievable means of access and preserving their own self-efficacy when they are concerned that *they* are the weakest link, is extremely challenging. This is compounded by a (not unwarranted) suspicion that the organisations offering them advice or security measures are biased by their own requirements, making it more onerous to evaluate what 'proportionate' cyber security should look like and reducing their access to effective controls.

There are four contributions made by this disseration that can already directly influence SSITUs' cyber security:

- **Describing the current state of play:** SSITUs are currently more motivated by their peers than by quantifiable risk, or their supply chain's needs. Chapters 4 and 5 provide SSITUs with the benchmark they requested: a description of both their peers' perceived risk, and current implementation of cyber security. This benchmark is significantly lower than that presented by Cyber Essentials [111] and aligns with suggestions from [41] for prioritising measures based on their efficacy. While this could be perceived as a negative by those publicising Cyber Essentials, we anticipate that there are large clusters of SSITUs isolated from other influencers, for whom the best motivation is knowing that breaches caused by a lack of antivirus, automatic updates, or 'strong' passwords will make them appear uninformed to their peers.

- **Describing the best practices capability gap:** for users with extremely limited technical knowledge the prospect of data protection regulations, or customers, questioning their cyber security practices and hinting at catastrophic risk is daunting. Communicating the difference between reasonable cyber security practices for SSITUs — proportionate, effective, etc. — and the common presentation of best practices is important. Telling a SSITU that 'being secure' depends on their applying a disproportionately expensive security measure to a system artefact or process that they *do not have* is counter-productive. Chapter 6 describes the constraints SSITUs typically operate within for those developing new solutions, but Chapters 4 and 5 keep those constraints in context, comparing them with common cyber security practices and providing insight to SSITUs.

- **Understanding self-efficacy:** we are not unique in highlighting the importance of self-efficacy in the decisions made by SSITUs [86, 87] and it is clear from our dataset that it is crucial that SSITUs maintain their self-efficacy and independence. While each organisation will have slightly differing requirements and cyber breaches will have different characteristics, a decision maker's reaction to their perceived inefficacy remains consistent. A decision maker's confidence does not change the amount of risk a security measure treats, but if that decision maker thinks it is no longer worth attempting cyber security then they may reduce the measures they implement and increase their risk. Without providing any additional training, or new measures, making SSITUs aware of this potential pitfall and asking them to scrutinise their reaction may contribute to their maintaining 'reasonable' security.

- **It allows SSITUs to become SPs for other SSITUs:** the SSITU marketplace is complex and it is likely that it will require both diverse technical solutions and an increase in the number of cyber security professionals offering support within local communities to have a significant impact on SSITU security. The requirements framework presented in Chapter 6 is an expensive artefact to produce, providing both marketing information and product design criteria. Making this framework openly available lowers the cost of entry for those wishing to develop cyber security solutions for SSITUs, enabling more SSITUs to enter the cyber security sector.

7.1.2 *Contributions to security providers*

We introduced this research by describing a gap in the cyber security marketplace; however, for this gap to be exploitable we need to show that there is a valid business case that could secure the support of cyber security providers.

Chapter 6 outlined two requirements frameworks for the SSITU ecosystem. We chose this approach, rather than one of communicating directly with SSITUs, because by generalising and structuring our results we hoped to make them more accessible to SPs and increase the reach of our research outcomes. This study will not contribute novel information to large cyber security incumbents, with their own customer base to mine for market-research data, however, we hope it is of value to less specialist SPs: large service providers who never intended to become a SP and for small, disruptive organisations wanting to change the marketplace.

The choice to focus a research study intended to improve SSITUs' engagement with cyber security on producing an artefact they are unlikely to directly use may seem counter-intuitive. However, SSITUs by nature are always going to be a group with limited knowledge and access to expertise. The majority are going to rely on security providers to set benchmarks and provide advice and products — where *awareness* projects nudge SSITUs, *accessibility* projects need to nudge the wider ecosystem and provide information to help the other stakeholder groups understand SSITUs' needs. SSITUs operate under so many constraints (from basic knowledge to control of their system) that influencing the way SPs approach this marketplace was going to help SSITUs improve their security more than they could achieve alone.

The first framework is successful in that it highlights that for SSITUs to achieve 'reasonable security' inside of their organisation they need solutions that preserve their self-efficacy well enough to become effective. It also highlighted the need for SSITUs to raise their baseline levels of security towards a benchmark so that their weakest link wasn't quite such low-hanging fruit. We are confident that the requirements framework for SSITU cyber security offers potential SPs an improved set of assumptions with which to kick-off a solution design process.

We believe there is demand for cyber security solutions that are "cheap, quick and easy to deploy" in the SSITU sector, which SSITU startups would be perfectly placed to exploit. There is a business case to develop solutions, but the portion of the system directly controlled by SSITUs limits this to a niche marketplace, potentially already saturated by antivirus and software firewall vendors. This may make it more effective for cyber security startups to focus on products that complement IT services offered by other suppliers (system elements uncontrolled by the SSITU), cultivating partnerships and potential purchasers for venture-capital led projects. For those aiming to interact directly with SSITUs, the gap in the marketplace is in the services sector — affordable support, training and expert advice — the maintenance of self-efficacy.

The contribution made by the second, supply chain focused, framework is discussed in more detail in Section 7.1.3.

7.1.3 *Contributions to risk-holders*

The message from RHs is clear — in order to maintain reasonable security within their own organisations they need to stop the SSITUs in their supply chains being both an attacker's available means of access and the weakest link. Their stake in the small-scale cyber security ecosystem is not to cultivate reasonable security in SSITUs; rather, it is to reduce their own risk.

Unfortunately, as outlined in Chapter 6, RHs' requirement for SSITUs to reduce the risk transferred to them neither represents proportionate security, nor resolves their lack of access to effective tools for the IT systems they implement. A summary of the arguments made in Chapter 6, presented as a cyber security cost-benefit analysis from the perspective of a SSITU, can be seen in Figure 48[1].

The value of the asset transferred to the SSITU by a large RH is irrelevant to their calculation of risk — their evaluation of risk will relate to the value of the contract with the RH and the likelihood of reputational damage or expensive litigation (both of which represent a catastrophic risk to the organisation, from which they cannot recover). The SSITU will consider 'proportionate security' to be in proportion to the contract's value — an order of magnitude in the hundreds or thousands — where the RH needs security proportionate to a risk of a magnitude in the hundreds of thousands or millions (recent ransomeware attacks having left several organisations with costs of up to $300Million[2]).

1 In comparing cyber security budgets against revenue Figure 48 makes the assumption that the SSITU is a mature business and the RH will pay in reasonable time, otherwise cyber security investment could create cash flow problems at a far lower value and the thresholds of influence adjust down accordingly.

2 www.bbc.co.uk/news/technology-41336086

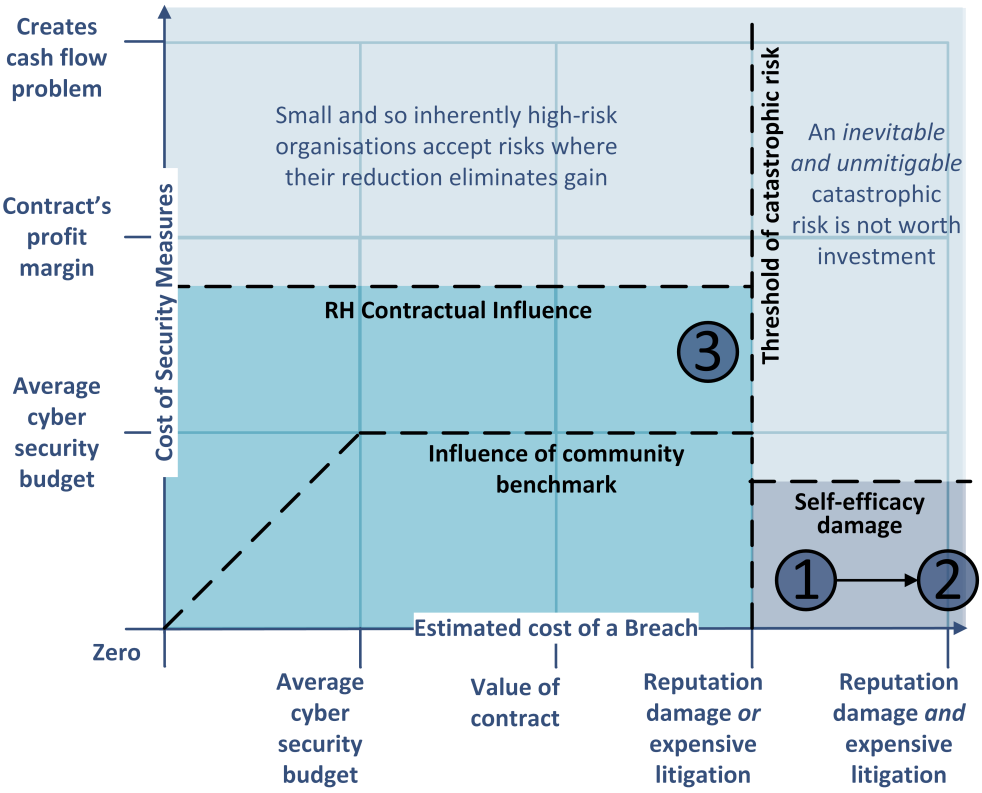


Figure 48: *Overview of SSITUs' cyber security cost-benefit analysis highlighting the difficulties the supply chain faces in encouraging cyber security engagement*

For this reason we approached the problem with the intention of:

1. Communicating the realities of SSITUs' operating environment to improve assumptions.

2. Separating the conflicting goals of SSITUs and the supply chain to give security providers the opportunity to develop effective controls.

The contribution made by the framework for supply chain cyber security is more marked than that of the framework for SSITUs. In accumulating and evaluating requirements the framework describes how SSITUs and RHs have conflicting definitions of proportionate security — it being unrealistic to expect SSITUs to protect assets that have far more value than the sum of the SSITU's own assets.

Having justified to RHs why the traditional approach of transferring risk to 'price takers', followed by attempts to enforce their contracts, was not going to succeed in this instance, we highlighted a subset of requirements that made the business case for RHs to take more ownership of supply chain security. Using Pfleeger and Pfleeger's principles to summarise: attackers are beginning to regard SSITUs as the point of 'easiest penetration' into RHs' systems. This represents an intangible reputational risk for the SSITU, but any tangible risk to the SSITU is likely to be an unintended consequence of the attack. They are likely to remain operational. However, the reputational damage of a breach is likely to be catastrophic to SSITUs ('1' in Figure 48) and their lack of influence over their suppliers and customers, combined with a lack of ability to achieve current cyber security best practices, means that their controls lack 'effectiveness'. They

are also, despite having far less access to experts, far less likely to be offered support by their suppliers or the UK Government — they are too small and numerous for support to be cost-effective. The lack of both effectiveness and support, while attempting to control *disproportionate* risk, acts to further undermine self-efficacy, further reducing SSITU engagement with security. This increases the inequality in achieved security between SSITUs and their supply chains, reinforcing their position as the 'weakest link'.

The supply chain has created a perfect storm for SSITUs, and (beyond the basics) only the supply chain can influence SSITUs' effectiveness.

SSITUs, SMEs in particular, require independence, so the requirements outlined in the framework for supply chain cyber security avoid RHs implementing security inside of SSITUs' systems. (The portion of the system controlled and directly securable by SSITUs is so insubstantial that most SSITUs have already implemented the available mitigations.) Instead, the requirements framework focuses on how RHs should change the status of SSITUs to produce an ecosystem of partnerships, influence the level of security and support the supply chain offers SSITUs, protect SSITUs' self-efficacy, and invest in increasing security equality across the supply chain. RHs do have some scope to influence the cyber security of their suppliers, but this is at point '3' in Figure 48: *before* a risk becomes catastrophic and within the profit margin of the contract (rather than enforcing a contract and moving from '1' to '2'). Ultimately, this indicates that for RHs to maintain reasonable security within a complex supply chain, they need to draw the lines of responsibility so that they are only transferring reducible risk onto SSITUs.

We suggest that RHs need to completely re-assess the way that they interact with their small suppliers before they will be able to manage supply chain cyber security risk. They need to invest in their supply chain partnerships and use their influence to generate support.

7.1.4 *Contributions to academia*

The research outcomes of this project have added data points into the academic literature [71, 72, 73, 74, 75, 76], which in some respects makes our contribution to academia more concrete than those described in Sections 7.1.1–7.1.3 — the time required to promote and prove research impact meaning that our contributions through outreach are ongoing.

There is another, methodological, contribution this study (alongside parallel publications [78, 86]) makes to academia. Part of the reason small-scale cyber security is under-researched is the lack of engagement of some user groups with research, most significantly, SMEs. As mentioned in Chapter 2, SMEs are a stakeholder group that are notoriously difficult to recruit [56, 127], with the domain of cyber security adding extra challenges [18].

However, our initial study [76] and the further outcomes described in Chapters 4–6 show how critical empirical research can be in helping experts make accurate assumptions about users' awareness and implementation of cyber security. Our study demonstrated that is is possible to engage SMEs in empirical cyber security research, during which we learned the following lessons:

- **Provide value:** where it's possible to recruit individuals with small financial incentives, business owners needed to see the value for their company of investing

in the research. Each participant was only asked for a small (in terms of time) contribution and was offered tailored information about the research outcomes in return; SMEs and large stakeholders were treated equally — our funding did not require us to preference a particular stakeholder; we had to network and interact with SMEs in the way that they interact with each other to gain access; and participating was personal — most of the business owners invested time in a researcher, not in building a relationship with the university brand.

- **Make participating convenient:** data collection methods often focus on controlling the environment, but inconveniencing already hard-to-recruit participants was going to alienate them. We met with participants in locations convenient to them — in some instances the participants worked from home and requested that the interview take place in the same café they used for business meetings. This did have the downside of us being unable to audio-record the meeting, as we would have also captured other conversations.

- **Make participating low impact:** we had to have enough flexibility in the research design for the business owners' own risk assessments and constraints on how they wanted to interact with us. One example of this was participants who chose not to be audio recorded, so that they could openly provide examples for context, while asking that these not be included in the dataset. Interacting with SME participants often amalgamates the processes of gaining permission from the organisation and gaining ethical consent from the individual.

We concluded that working with small organisations was entirely about adapting the research design to fit with that group's existing working practices and ensuring that we invested enough in our participants to allow them to see a return on their investment.

The outcomes of the survey this approach facilitated hint at several directions for future research to take, which we discuss in Section 7.3. Chapter 6 also contributes global business requirements and constraints to technical specialists researching and developing new solutions. However, there are some obvious limitations to this work, which we discuss in Section 7.2.

7.2 PROJECT LIMITATIONS

As with every research project, this study has its limitations. The obvious place to begin this discussion is with an evaluation of the methodology we selected.

We chose a qualitative method, so, as described in Chapter 3, we intended to collect sample that quantitative researchers would not consider of high enough volume to present significant findings. The analysis method was inductive and self-validating.

Although certain audiences for our research may have been more receptive to a quantitative study, we have successfully presented insight into the constraints faced by SSITUs. However, the method we have used is intended to identify *themes*. In Chapter 6 we organised, structured and analysed those themes to produce an artefact we hope will be usable and impactful outside of the academic community. What the project hasn't achieved is a validation that our understanding of the SSITU group can trans-

late into the production of specific tools — the DPhil scope necessitated moving this experiment into the 'future work' category.

The identification of themes also leaves more detailed data collections and analyses for future projects. For example, we were able to identify multi-purpose devices, low-infrastructure IT strategies and limited cyber security knowledge as themes within the SSITU user group. However, we cannot provide statistics relating to the proportion of SSITUs who identify with one (or all three) of these themes, or the exact technologies they employ for these purposes.

The use of theoretical (rather than random) sampling when recruiting participants does have one downside — we, and a number of our participants, suspect that there are large networks of SSITUs isolated from the cyber security ecosystem. To be able to recruit our participants we had to network with SSITUs, resulting in a participant group who are at most two degrees of separation from a cyber security expert. Given the preponderance of consumer technologies and extremely low technical literacy described by some of our participants it is unlikely that this has led to a failure to identify themes these isolated groups would identify with. But there is always a risk that this inaccessible group could have offered additional insights.

Publications since 2016 have offered alternative methods for engaging SMEs in research, and Renaud [86], despite mentioning the importance of building relationships with SMEs in her pilot study, eventually achieved a random sample of SME questionnaire respondents. The difference between our own study and Renaud's, or other large scale surveys [110, 49], is financial. Extrapolating from Renaud's methodology and reported response rate [86], or considering the marketing costs of a study led by a large consultancy [110, 49], the cost of a large-scale quantitative study would be significant.

In contrast, a smaller sample using ethnographic data collection could have provided far more in-depth knowledge about the decisions small organisations make around cyber security and helped us to understand how decisions are made when there is a clear conflict of interest. An Action Research approach [98] could also have provided a more advanced research outcome, allowing us to validate our knowledge of the sector by evaluating SSITU-specific security solutions in participant organisations. However, while the SSITUs needed an investment of our time before they would engage at all, they were limited in the level of engagement they were able to offer. More intrusive methods, such as collecting data by observation and interventional studies, ran a high risk of disrupting a small organisation's operation.

Providing the flexibility to SSITU participants we mentioned in Section 7.1.4 also limits the data we will be able to pass on to future projects — our interview transcriptions from field notes, taken during and just after interviews, cannot replace full audio transcripts. The continuity of the same researcher carrying out both interview and analysis may mean that it may be difficult for another researcher to take our raw dataset and produce the same results. However, any issues with the repeatability of this study can hopefully be overcome by the similarities between our results and those of concurrent projects [78, 86], as well as the evolution of UK Government dialogue around small-organisational security so that it is converging with the suggestions this study has made.

A mistake we made was in the way we requested ethical approval. To gain ethical approval the anonymity of all participants has to be guaranteed. Consequently, when interacting with very small organisations where business owners often have multiple

ventures, we needed to completely hide the identity of the organisation(s) to protect the identity of the participant. By not differentiating how we treated participants from other stakeholder groups during this process we hid the identity of any organisation who had participated. In the very small government community this made networking to recruit participants more challenging than it would normally have been.

We also struggled to recruit security providers in the private sector. Organisations for whom security was a requirement but not a primary selling point (operating systems, web development, IT service providers, etc.) were easy to recruit. SSITU-recognisable brands selling endpoint cyber security products were impossible to recruit. The need for SSITUs to have an unbiased researcher and publicly available research outcomes conflicts with the typical disclosure constraints of private sector collaboration agreements. In this case we have had to collect open-source data about products and services, rather than gaining active participation.

Finally, at the inception of this project we anticipated a cross-disciplinary study, but the outcomes of the survey led us into some unexpected domains. We did not expect the conflict between cyber security and privacy to become so prominent, nor did we expect to be putting so much emphasis on decisions made by the supply chain rather than independently by the SSITUs, and many of our requirements hinge on metrics that the research community may suggest are hard to produce [81].

7.3 FUTURE WORK

The outcomes of this research and the themes we have presented open a number of research areas for exploration:

- Can better cyber security tools be developed for the SSITU sector?
- Studying how pervasive BYOD models and low-infrastructure systems are in the SSITU sector, a measure of their growth and a better understanding of how this interacts with cyber security practices.
- An analysis of the dual roles SSITUs have within a supply chain: their commercial role as a price-taker versus their influential role in cyber security. Can the supply chain adapt to allow SMEs to be significant and insignificant at the same time?

For our part, using the framework to develop tools for SSITUs, or their supply chains, is an obvious next step. It would also be interesting to collect more data about SSITUs as organisations begin to comply with the GDPR and spend more time exploring the conflicts between privacy and cyber security at a personal level. Is the advice offered by the UK Government through their Cyber Essentials initiative sufficient to enable individuals to comply with data protection requirements? How much data does a malicious party need to steal an identity? Comparably, what proportion of this data are individuals required to publicly disclose to incorporate a company? How much does it cost to separate a business' public identity from the individual's private one and what impact does this have on other cyber security investment?

Also relevant, given the lessons we learned throughout this project, is the approach we intend to take in this next phase of research. Small-scale partnerships with SME participants on small projects have worked and any applications for future funding will need continual engagement from SMEs.

Working with SMEs places constraints on the pace of the project — they cannot usually guarantee their availability 3-6 months from the point of proposal and need to be able to complete work packages at a faster pace than their academic counterparts. For SMEs to see a return on the time they invest they also need to play a significant role in a project. This makes accessing government funds challenging given the evolution towards large inter-organisational grants — an SME with an annual turnover equivalent to the annual cost of an academic researcher would become invisible in one of these consortia and may struggle to assert their ownership of any intellectual property their research produces.

Our future projects and the research questions we address will be influenced by the partnerships it is possible to create.

7.4 CONCLUSION

Requirements exist, irrespective of whether or not they have been identified. Up until recently the expectation of the cyber security community has been that they could scale-down their experience to fit SSITUs and that their cyber security risks and requirements would be trivial. What is becoming increasingly obvious is that small-scale cyber security is just as complex and challenging as its large-scale counterpart. Except that SSITUs are working without a clear roadmap, with best practices that are unsuited to their organisation, an uncooperative supply chain and no knowledge or funds. And when a large risk holder traces potential attack vectors, they often find a SSITU.

BIBLIOGRAPHY

[1] Def Stan 00-56. *Interim Defence Standard 00-56 Part 1*. Ministry of Defence, UK, February 2014.

[2] BS EN ISO 16484-5:2012. *Building automation and control systems*. British Standards Institute, London, UK, 2012.

[3] ISO/IEC 27000:2016. *Information technology — Security techniques — Overview and vocabulary*. International Standards Organization, Geneva, Switzerland, 2016.

[4] ISO/IEC 27001:2017. *Information technology — Security techniques — Information security management systems requirements*. International Standards Organization, Geneva, Switzerland, 2017.

[5] ISO/IEC 27002:2013. *Information technology — Security techniques — Code of practice for information security controls*. International Standards Organization, Geneva, Switzerland, 2013.

[6] ISO/IEC 27005:2017. *Information technology — Security techniques — Information security risk management*. International Standards Organization, Geneva, Switzerland, 2017.

[7] BS ISO/IEC 27011:2008. *Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*. British Standards Institute, London, UK, 2008.

[8] PD ISO/IEC TR 27019:2013. *Information technology – Security techniques – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry*. British Standards Institute, London, UK, 2013.

[9] ISO/IEC 31000:2009. *Risk management*. International Standards Organization, Geneva, Switzerland, 2009.

[10] BS EN 60950-1:2006+A2:2013. *Information technology equipment – Safety – General requirements*. British Standards Institute, London, UK, 2013.

[11] Adaptly, Refinery29, and Facebook. The science of social media advertising — a research study on sequenced for call to action vs. sustained call to action. `www.facebook.com/business/news/value-of-storytelling-on-facebook`, 2014.

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

[13] Christopher Alberts and Audrey Dorofee. *Managing Information Security Risks: The OCTAVE Approach*. Addison Wesley, 2003.

[14] Meg Leta Ambrose. It's about time: Privacy, information life cycles, and the right to be forgotten. *Stanford Technology Law Review*, 16:369–422, 2012.

[15] Nadya Bartol. Cyber supply chain security practices DNA – Filling in the puzzle using a diverse set of disciplines. *Technovation*, 34(7):354–361, 2014.

[16] Hilary Berger and Andrew Jones. Cyber security & ethical hacking for SMEs. In *Proceedings of the The 11th International Knowledge Management in Organizations Conference on The Changing Face of Knowledge Management Impacting Society*, 2016.

[17] Peter M Blau. A formal theory of differentiation in organizations. *American Sociological Review*, 35:201—218, 1970.

[18] Shawn Butler. Security design: Why it's hard to do empirical research. In *Workshop on Using Multidisciplinary Approaches in Empirical Software Engineering Research, affiliated with the 22nd International Conference on Software Engineering (ICSE 2000)*, 2000.

[19] Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, James Broberg, and Ivona Brandic. Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation computer systems*, 25 (6):599–616, 2009.

[20] Richard A. Caralli, James F. Stevens, Lisa R. Young, and William R. Wilson. Introducing OCTAVE Allegro: Improving the information security risk assessment process. Technical report, Software Engineering Institute, Carnegie Mellon University, 2007.

[21] John Carroll. *Computer Security*. Butterworth-Heinemann, 2nd edition, 1987.

[22] John Carroll. *Computer Security*. Butterworth-Heinemann, 3rd edition, 1996.

[23] K. Charmaz. *Constructing Grounded Theory*. Sage, 2nd edition, 2014.

[24] Robert B. Cialdini. Crafting normative messages to protect the environment. *Current Directions in Psychological Science*, 12(4):105–109, 2003.

[25] Committee on National Security Systems. National information assurance (IA) glossary, 2010.

[26] Juliet Corbin and Anselm Strauss. *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage, 3rd edition, 2008.

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

[28] UK Government Department for Business, Energy & Industrial Strategy. Business population estimates for the UK and regions 2016. `www.gov.uk/government/statistics/business-population-estimates-2016`, 2016.

[29] K. Dörnemann and A. von Gernler. Cybergateways for securing critical infrastructures. In *Security in Critical Infrastructures Today: Proceedings of International ETG-Congress 2013*, 2013.

[30] Florian Egloff. Cybersecurity and the age of privateering: A historical analogy. Technical report, University of Oxford, 2015.

[31] Kathleen Eisenhardt. Building theories from case study research. *The Academy of Management Review*, 14(4):532–550, 1989.

[32] European Commission. Commission Recommendation concerning the definition of micro, small and medium-sized enterprises (C(2003) 1422). eur-lex.europa.eu/legal-content/EN/TXT/?qid=1503161336347&uri=CELEX:32003H0361, 2003.

[33] European Union Agency for Network and Information Security. Information packages for small and medium sized enterprises (SMEs) - ENISA. www.enisa.europa.eu/publications/information-packages-for-small-and-medium-sized-enterprises-smes, 2006.

[34] Andrew Fielder, Emmanouil Panaousis, Pasquale Malacaria, Chris Hankin, and Fabrizio Smeraldi. Decision support approaches for cyber security investment. *Decision Support Systems*, 86:13–23, 2016.

[35] Ivan Flechais, M. Angela Sasse, and Stephen M. V. Hailes. Bringing security home: A process for developing secure and usable systems. In *Proceedings of the 2003 Workshop on New Security Paradigms*, 2003.

[36] Tom Gilb. *Competitive Engineering*. Elsevier Butterworth-Heinemann, 2005.

[37] Robin Goldsmith. *Discovering Real Business Requirements for Software Project Success*. Artech House, 2004.

[38] Adam Gordon. *The official* $(\mathrm{ISC})^2$ *guide to the CISSP CBK*. Taylor Francis, 2015.

[39] G. Guest, A. Bunce, and L Johnson. How many interviews are enough? An experiment with data saturation and variability. *Field Methods*, 18(1):59–82, 2006.

[40] Craig Heffner and Derek Yap. Security vulnerabilities in SOHO routers. www.exploit-db.com/docs/252.pdf, 2009.

[41] Chad Heitzenrater and Andrew Simpson. Policy, statistics and questions: Reflections on uk cyber security disclosures. *Journal of Cybersecurity*, 2(1):43–56, 2016.

[42] Cormac Herley. So long, and no thanks for the externalities: The rational rejection of security advice by users. In *Presented at the New Security Paradigms Workshop (NSPW)*, 2009.

[43] Cormac Herley. More is not the answer. In *IEEE Security and Privacy magazine*, 2014.

[44] Joseph W Jerome. Buying and selling privacy: Big data's different burdens and benefits. *Stanford Law Review Online*, 66:47, 2013.

[45] Yvonne Jewkes. *Crime Online*. Routledge, 2013.

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

[47] S. Karnouskos. Smart houses in the smart grid and the search for value-added services in the cloud of things era. In *Proceedings of the 14th IEEE International Conference on Industrial Technology (ICIT 2013)*. IEEE, 2013.

[48] Lori M Kaufman. Data security in the world of cloud computing. *IEEE Security & Privacy*, 7(4):61–64, 2009.

[49] KPMG and Cyber Aware. Small business reputation and the cyber risk. www.cyberaware.gov.uk/sites/cyberstreetwise/files/cyber_streetwise_kpmg_-_small_business_reputation_report_final.pdf, 2016.

[50] E. Kritzinger and S H von Solms. Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, 29:840–847, 2010.

[51] Edward P. Lazear. Entrepreneurship. *Journal of Labor Economics*, 23(4):649–680.

[52] Gwanhoo Lee and Weidong Xia. Organizational size and it innovation adoption: A meta-analysis. *Information & Management*, 43(8):975–985, 2006.

[53] N. G. Leveson. *Safeware: System Safety and Computers*. ACM, 1995.

[54] Riyana Lewis, Panos Louvieris, Pamela Abbott, Natalie Clewley, and Kevin Jones. Cybersecurity information sharing: A framework for sustainable information security management in UK SME supply chains. In *Proceedings of ECIS 2014*, 2014.

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

[56] Nigel Lockett and David H. Brown. Aggregation and the role of trusted third parties in SME e-business engagement — a regional policy issue. *International Small Business Journal*, 24(4):379–404, 2006.

[57] Jonathan Lusthaus. How organised is organised cybercrime? *Global Crime*, 14(1): 52–60, 2013.

[58] Mary Madden, Susannah Fox, Aaron Smith, and Jessica Vitak. Digital footprints — online identity management and search in the age of transparency. Technical report, Pew Research Center, 2007.

[59] Pratyusa K Manadhata and Jeannette M Wing. An attack surface metric. *IEEE Transactions on Software Engineering*, 37(3):371–386, 2011.

[60] Kirsten Martin and R. Edward Freeman. Some problems with employee monitoring. *Journal of Business Ethics*, 43(4):353–361, 2003.

[61] Susan McGregor, Polina Charters, Tobin Holliday, and Franziska Roesner. Investigating the computer security practices and needs of journalists. In *In Proceedings of the 24th USENIX Security Symposium*, 2015.

[62] Keith W Miller, Jeffrey M Voas, and George F Hurlburt. Byod: Security and privacy considerations. *It Professional*, 14(5):53–55, 2012.

[63] R. Mitchell and I.-R. Chen. A survey of intrusion detection techniques for cyber-physical systems. *ACM Computing Surveys*, 46(4):55:1–55:29, 2014.

[64] Arvind Narayanan and Vitaly Shmatikov. Robust de-anonymization of large sparse datasets. In *Proceedings of the IEEE Symposium on Security and Privacy*, 2008.

[65] National Institute of Standards and Technology. NIST cybersecurity framework. `www.nist.gov/document-3766`, 2014.

[66] Marcus Niemietz and Jörg Schwenk. Owning your home network: Router security revisited. In *Proceedings of the 9th Workshop on Web 2.0 Security and Privacy (W2SP) 2015*, 2015.

[67] Institute of Chartered Accountants in England and Wales. *Chartech Cyber Security: 10 steps to cyber security for the smaller firm*. ICEAW, 2013.

[68] Institute of Chartered Accountants in England and Wales. *Audit Insights: Cyber Security 2015*. ICEAW, 2015.

[69] P. Ohm. Broken promises of privacy: Responding to the surprising failure of anonymization. In *University of Colorado Law Legal Studies Research Paper*, 2009.

[70] Emma Osborn. Business versus technology: Sources of the perceived lack of cyber security in SMEs. Technical report, University of Oxford, 2014.

[71] Emma Osborn and Andrew Simpson. Small-scale cyber security. In *Proceedings of the 2nd International IEEE CSCloud Conference*, 2015.

[72] Emma Osborn and Andrew Simpson. On safety and security requirements in emerging ubiquitous computing models. *The Computer Journal*, 59(4):570–591, 2016.

[73] Emma Osborn and Andrew Simpson. On small-scale IT users' system architectures and cyber security: A UK case study. *Computers & Security*, 70:27–50, 09 2017.

[74] Emma Osborn and Andrew Simpson. A requirements framework for small-scale cyber security. *In preparation*, 10 2017.

[75] Emma Osborn and Andrew Simpson. Risk and the small-scale cyber security decision-making dialogue — a UK case study. *Accepted by The Computer Journal*, 04 2017.

[76] Emma Osborn, Sadie Creese, and David Upton. Business versus technology: Sources of the perceived lack of cyber security in SMEs. In *Proceedings of the 1st International Conference on Cyber Security for Sustainable Society*, 2015.

[77] Oxford University Press. *Oxford English Dictionary*. Referenced 2016, continuously updated.

[78] Simon Parkin, Andrew Fielder, and Alex Ashby. Pragmatic security: Modelling it security management responsibilities for sme archetypes. In *Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats*, 2016.

[79] A. Pfitzmann. Why safety and security should and will merge. In *Proceedings of the 23rd International Conference on Computer Safety, Reliability, and Security (SAFECOMP 2004)*, 2004.

[80] Charles P. Pfleeger and Shari Lawrence Pfleeger. *Security in Computing*. Prentice Hall, 4th edition, 2007.

[81] Shari Pfleeger and Robert Cunningham. Why measuring security is hard. *IEEE Security & Privacy*, 8(4):46–54, 2010.

[82] L. Piètre-Cambacédès and M. Bouissou. Cross-fertilization between safety and security engineering. *Reliability Engineering & System Safety*, 110:110–126, 2013.

[83] L. Piètre-Cambacédès and C. Chaudet. The SEMA referential framework: Avoiding ambiguities when dealing with security and safety issues. *International Journal of Critical Infrastructure Protection*, 3(2):55–66, 2010.

[84] Teri Radichel. Case study: Critical controls that could have prevented target breach. Technical report, SANS Institute InfoSec Reading Room, 2014.

[85] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic. Cyber-physical systems: The next computing revolution. In *Proceedings of the 47th ACM/IEEE Design Automation Conference (DAC 2010)*, 2010.

[86] Karen Renaud. How smaller businesses struggle with security advice. *Computer Fraud & Security*, 2016(8):10–18, 2016.

[87] Hyeun-Suk Rhee, Cheongtag Kim, and Young U. Ryu. Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, 28(8):816–826, 2009.

[88] H.W.J. Rittel and M.M. Webber. Dilemmas in a general theory of planning. *Policy Sciences*, 4(2):155–166, 1973.

[89] Jeffrey Ritter. *Achieving digital trust: new rules for business at the speed of light*. Self-published, 2015.

[90] Suzanne Robertson and James Robertson. *Mastering the Requirements Process*. Addison Wesley, 3rd edition, 2013.

[91] Bruce Schneier. A taxonomy of social networking data. *IEEE Security & Privacy*, 8(4):88, 2010.

[92] John Scott-Railton. Security for the high-risk user: Separate and unequal. *IEEE Security and Privacy*, 14(2):79–87, 2016.

[93] D. N. Serpanos and A. G. Voyiatzis. Security challenges in embedded systems. *ACM Transactions on Embedded Computing Systems*, 12(1s):66:1–66:10, 2013.

[94] Q. Shafi. Cyber physical systems security: A brief survey. In *Proceedings of the 12th International Conference on Computational Science and Its Applications (ICCSA 2012)*, Salvador de Bahia, Brazil, 2012.

[95] Ian Somerville and Pete Sawyer. *Requirements Engineering: a Good Practice Guide*. Wiley, 1997.

[96] Frederick Stier. *Research and Reflexivity*. Sage, 1991.

[97] N. Storey. *Safety-Critical Computer Systems*. Addison Wesley, 1996.

[98] Ernest T. Stringer. *Action Research*. Sage, 1999.

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

[100] The European Commission. The 'Blue Guide' on the implementation of EU product rules 2016. ec.europa.eu/DocsRoom/documents/18027, 2016.

[101] The European Parliament and The Council of The European Union. Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data. ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf, 1995.

[102] The European Parliament and the Council of the European Union. Directive 2001/95/EC on general product safety. eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32001L0095, 2001.

[103] The European Parliament and The Council of The European Union. General Data Protection Regulation. eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679, 2016.

[104] Daniel R. Thomas, Alastair R. Beresford, and Andrew Rice. Security metrics for the android ecosystem. In *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices*, 2015.

[105] UK Government — Charity Commission for England and Wales. Recent charity register statistics: Charity Commission. www.gov.uk/government/publications/charity-register-statistics/recent-charity-register-statistics-charity-commission, Referenced 2017, continuously updated.

[106] UK Government — Government Equalities Office. Private clubs and associations: quick start guide. www.gov.uk/government/publications/private-clubs-and-associations-quick-start-guide, 2011.

[107] UK Government. Data Protection Act 1998. www.legislation.gov.uk/ukpga/1998/29, 1998.

[108] UK Government. Charities act 2011. www.legislation.gov.uk/ukpga/2011/25, 2011.

[109] UK Government. The UK cyber security strategy: Protecting and promoting the UK in a digital world. www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf, 2011.

[110] UK Government. Information security breaches survey 2013. www.gov.uk/government/publications/information-security-breaches-survey-2013-technical-report, 2013.

[111] UK Government. Cyber Essentials Scheme: Requirements for basic technical protection from cyber attacks. www.gov.uk/government/publications/cyber-essentials-scheme-overview, 2014.

[112] UK Government. 10 steps to cyber security. www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary, 2015.

[113] UK Government. Consumer rights act 2015. www.legislation.gov.uk/ukpga/2015/15, 2015.

[114] UK Government. Data protection summary. www.gov.uk/data-protection/the-data-protection-act, 2016.

[115] UK Government. National cyber security strategy 2016 to 2021. www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf, 2016.

[116] UK Government. The UK cyber security strategy 2011-2016 - annual report 2016. www.gov.uk/government/publications/the-uk-cyber-security-strategy-2011-2016-annual-report, 2016.

[117] US International Trade Commission. Small and medium-sized enterprises: Overview of participation in US exports. www.usitc.gov/publications/332/pub4125.pdf, 2010.

[118] Michel Van Eeten and Johannes M. Bauer. Emerging threats to internet security: Incentives, externalities and policy implications. *Journal of Contingencies and Crisis Management*, 17(4):221–232, 2009.

[119] Michel Van Eeten and Johannes M. Bauer. Enhancing incentives for internet security. In *Research handbook on governance of the internet*, pages 445–484. Edward Elgar Publishing, 2013.

[120] Heidi Vandebosch and Katrien Van Cleemput. Defining cyberbullying: A qualitative research into the perceptions of youngsters. *Cyberpsychology & Behaviour*, 11(3):499–503, 2008.

[121] Rossouw von Solms and Johan van Niekerk. From information security to cyber security. *Computers & Security*, 38:97–102, Oct 2013.

[122] Stephen D. Weaver and Mark Gahegan. Constructing, visualizing, and analyzing a digital footprint. *Geographical Review*, 97(3):324–350, 2007.

[123] Barry Wellman, Janet Salaff, Dimitrina Dimitrova, Laura Garton, Milena Gulia, and Caroline Haythornthwaite. Computer networks as social networks: Collaborative work, telework, and virtual community. *Annual Review of Sociology*, 22: 213–238, 1996.

[124] Karl Wiegers and Joy Beatty. *Software Requirements*. Microsoft Press, 3rd edition, 2013.

[125] T. Wolf, M. Zink, and A. Nagurney. The cyber-physical marketplace: A framework for large-scale horizontal integration in distributed cyber-physical systems. In *Proceedings of the 33rd IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW 2013)*, 2013.

[126] G. Wondracek, T. Holz, E. Kirda, and C. Kruegel. A practical attack to de-anonymize social network users. In *In Proceedings of the 2010 IEEE Symposium on Security and Privacy*, 2010.

[127] Steve Woolgar. Social basis of interactive social science. *Science and Public Policy*, 27(3):165–173, 2000.

[128] Michael Workman. Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, 59(4):662–674, 2008.

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

[130] Y. Yan, Y. Qian, H. Sharif, and D. Tipper. A survey on smart grid communication infrastructures: Motivations, requirements and challenges. *IEEE Communications Surveys & Tutorials*, 15(1):5–20, 2013.

[131] Ebru Yeniman Yildirim, Gizem Akalp, Serpil Aytac, and Nuran Bayram. Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management*, 31(4):360–365, 2011.

[132] Iryna Yevseyeva, James Turland, Charles Morisset, Lynne Coventry, Thomas Groß, Christopher Laing, and Aad van Moorsel. Addressing consumerisation of it risks with nudging. *International Journal of Information Systems and Project Management*, 3(3):5–22, 2015.

[133] John Zimmerman, Jodi Forlizzi, and Shelley Evenson. Research through design as a method for interaction design research in HCI. In *In Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM, 2007.

[134] Dimitrios Zissis and Dimitrios Lekkas. Addressing cloud computing security issues. *Future Generation computer systems*, 28(3):583–592, 2012.

A

APPENDIX A – QUESTIONNAIRE PRESENTED TO SMES

ABOUT YOUR COMPANY

1. **What is your role within your company?**
2. **What industry sector is your company in?**
3. **Does your company have dedicated offices?** *(yes; no)*
4. **Which county is your company based in?** *(option list)*

THE SIZE OF YOUR COMPANY

5. **How many people work at your company (including company directors etc.)?** *(just me; more than 1, less than 10; 10 or more, less than 50; 50 or more, less than 250; 250 or more)*
6. **What is your estimated annual turnover?** *(less than £79,000; £79,000 or more, less than £1.6million; £1.6million or more, less than £8.2million; £8.2milion or more, less than £41million; £41million or more)*

ABOUT YOUR COMPANY'S TECHNOLOGY USE & BUDGETS

7. **Average number of computers containing work files etc. per person?** (Excludes tablets & mobile phones. Includes looking at work emails on a home computer for example) *(0; 1; 2; 3 or more)*
8. **Average number of smartphones or tablets containing work files etc. per person?** (Including looking at work emails on a personal device for example) *(0; 1; 2; 3 or more)*
9. **How much do you currently spend per year on cyber security, including antivirus, firewalls, staff training etc. (£)?** *(Nothing; £100 or less; £100 to £499; £500 to £999; £1,000 to £4,999; £5,000 to £9,999; £10,000 to £49,000; £50,000 to £99,000; £100,000 or more)*
10. **If a significant number of SMEs were adopting a cyber security standard, allowing companies to become accredited for handling cyber security well, when would the set-up cost become unaffordable for your company?** *(£500 or less; £500 to £999; £1,000 to £4,999; £5,000 to £9,999; £10,000 to £49,000; £50,000 to £99,000; £100,000 to £999,999; £1million or more)*
11. **Does your company have a website?** *(yes; no)*

YOUR CYBER SECURITY KNOWLEDGE AND AWARENESS

12. **Please rate how these statements apply to you** *(Strongly Agree; Agree; Neither Agree or Disagree; Disagree; Strongly Disagree)*
    a) I don't know what cyber security is
    b) I don't care what cyber security is
    c) Someone has made me think cyber security might be important
    d) The press have made me worried about cyber security
    e) I have done some reading about cyber security online
    f) I feel confident that I can maintain a suitable level of cyber security whilst I work
    g) I have someone I trust who can provide information about cyber security when needed
    h) I have thought about cyber security and decided it's out of my budget

MINI RISK ASSESSMENT

13. **Please rate how these statements apply to your company** *(Strongly Agree; Agree; Neither Agree or Disagree; Disagree; Strongly Disagree)*
    a) We have customer or supplier data that we need to protect
    b) We have intellectual property that we need to protect
    c) We have suppliers or customers who provide a link into their IT systems, or who we allow to link into ours
    d) We have lost / may lose customers because they are beginning to request that we are that we are certified with security standards (i.e. ISO 27001, PCI-DSS, IASME)
    e) Company sales are heavily dependent on the company and its employees maintaining a good reputation
    f) We have a website which allows people to login or input information into forms
    g) Using social media or recommendation websites is our main source of advertising (Linkedin, Twitter, RatedPeople.com etc.)
    h) We have safety critical systems (impacting on health and safety) accessed or controlled by our computers/mobile phones

14. **Please list any specific reasons that you think your company will come under attack**

BEHAVIOUR AND CURRENT CYBER SECURITY MEASURES

15. **Are these statements true or false in your company?** *(true; false; don't know)*
    a) People at my company use Facebook, LinkedIn, and Twitter etc. for advertising, job applications or organising social events.
    b) Some or all people at my company have a computer or smart phone issued to them
    c) People have the ability to install anything they wish on their work computers irrespective of company policy
    d) Anyone at work can access any file on company shared file servers
    e) People use webmail accounts (Gmail, Hotmail etc.) for work
    f) I have seen people's passwords for work systems written down around the office
    g) I let my children play with my my work phone or tablet and choose what apps to install

h) The company favours use of free or open source software
i) The company has its own social media account
j) The company have dedicated IT support staff to set up our computers
k) People use their own or customer USB sticks to exchange files at work
l) The company uses cloud services to store data or use applications (including Dropbox etc.)
m) Our computers have antivirus software and allow Windows (or equivalent) to auto-update
n) All our files are backed up and stored somewhere else in case there's a fire
o) The company has done an in-depth risk analysis which included cyber security
p) The company's risk analysis, policies and backups are kept up to date
q) The company is ISO 27001 certified
r) All the doors and windows are locked when the office is empty

YOUR CYBER SECURITY REQUIREMENTS

16. **Please mark how important each cyber security issue is to you.** Please include those already implemented and any which are on your cyber security wish list. *(critical; important; optional; not useful; I don't know what this is)*
    a) Basic Knowledge and Good Practice
    b) Disaster Recovery & Backups
    c) Resilience
    d) Cyber Security Standards
    e) Compliance for Insurance
    f) Physical Security of Equipment
    g) Reputation & Social Media
    h) End Point (Computer/Server) Security
    i) Smartphone or Tablet Security
    j) Network Security
    k) Website Security
    l) Security in the Cloud
    m) Cyber Incident Management

17. **Please mark the types of requirement you have for the issues you highlighted in the last question. You can select as many options as you like. Please include those already in place and any which are on your cyber security wish list.**

This section was filtered to show only items that respondents marked as critical, important or optional in question 16. For each issue they highlighted they could choose from the following six requirement types: advice guides; awareness training; consultancy; dedicated staff; implemented policy and implemented technology.

18. **Please list any requirements not mentioned in the last section that you need for good cyber security.**

19. **What do you find most difficult about Cyber Security?**

B

APPENDIX B – CONSUMER CPS SCENARIOS

SCENARIO 1: A 'SMART' REFRIGERATOR

Jen has a state-of-the-art refrigerator. When it was delivered, the technician connected it to Jen's home Wi-Fi network. The technician set up an account for her on the company's web-site and told her that she should log in to finish registering and look at the services she could use. The site gave her proof of purchase for the warranty, asked her if she wanted the refrigerator to automatically update its systems, and offered a remote-monitoring application plus some third party services. Through the recommended services, Jen was able to link the refrigerator's in-built food recognition system to her supermarket shopping application, allowing her shopping list to auto-update when she was running out of her favourite foods. The monitoring application provides information about the food she has in her refrigerator, alerting her when an item is about to go out of date or if the refrigerator isn't keeping the food cool enough. Jen also uses an application that automatically uploads information from her refrigerator into a diet diary so that she can keep an eye on the calories she consumes.

SCENARIO 2: A HOME CLIMATE-CONTROL SYSTEM

Jen's building has a sophisticated climate-control system. When she moved into her flat, as well as the keys, the landlord passed on the details for logging on to the manufacturer's web page. By logging in, Jen was able to change the climate-control settings on a room-by-room basis and download an application to allow her to turn on the heating in her house remotely. The application gave her the option of linking to her car's satellite navigation system so that when she selected the 'home' location, the climate-control system could automatically detect when Jen was close to home and turn the heating on. As well as linking to applications and the company web-site, the system links to the building's fire alarm system periodically providing health reports to help the alarm system detect faults before they become critical.

SCENARIO 3: AN IN-CAR MEDIA SYSTEM

Jen has also bought an application that is compatible with her car. Once downloaded, the application allows her tablet or phone to connect to the in-car system via Wi-Fi. Previous iterations of the product were sold as hardware and wired in to cars. Among other things, the system lets Jen have access to all her music through the dashboard screens. She finds a video on-line explaining how to install it and, once it is installed, she links her accounts so that her sat-nav can automatically look in her contacts to find the addresses she's travelling to, and letting her access music and videos through the in-car screens. The application also provides options for optimising engine control settings to the user's driving style (which Jen leaves for another day).

C

APPENDIX C – THE COMPLETE CODING TABLE

This appendix presents the full version of the coding table summarised in Chapter 3.

In addition to the phenomena, concepts and codes presented in the methodology it includes:

- In blue, the data fragments that contributed to each code, labelled with both the stakeholder group they represent and the interview number, or in some cases a label relating to the supplementary documentation the participant(s) provided or suggested for inclusion in the study.
- In grey italics, the memos generated by the analysis.
- Memos labelled MP1 or MP2 relate to findings from the CDT mini-projects that proceeded this analysis, so that results from these studies could be aligned with new findings.

Table 19: *Full coding table*

Phenomenon	Concepts	Codes	Data Fragments and *Memos*
Small Scale IT User Profile			WB_internet_2015 Internet penetration growing yearly
			WB_internet_2015 over 80% of the population of the developed world online
			WB_employment_2015 UK around 60% of over 15s employed
			Pervasive use of IT by small-scale IT users
			The proportion of UK residents having experienced cyber security training in the workplace relatively low
			Large user group with low resources and maladapted marketplace
			Defined by the fact they're not large well-resourced entities
			No single user group with coherent requirements
			No mutually exclusive user group (user groups image)
			Blur between groups impacts knowledge and attitude
	SSITUs	SME	EC_2014 99% of European businesses are SMEs
			EC_2003 definition of SME
			BIS_2013 SMEs account for 59.3% of employment and 48.1% of turnover in 2013
			USITC_2010 No single definition in US, but majority stating >500 employees
			Definition of 'small' inconsistent in different jurisdictions
		Charity	*can be comparable size but reason to operate is different*
			different decision making for cyber security
			potential for higher number of vulnerable customers
		Individuals not connected to large stakeholder	*Individual beliefs important in how users construct their privacy requirements*
			Overlap - privacy and cyber security for the individual
		Families	*Cyber footprint has a big overlap with personal cyber footprint but is distinct*
			Shared infrastructure, online services and decision making to protect vulnerable users
			Nominated technical 'expert'
			Shared cyber footprint may not be reflected in the material world
	Other Stakeholders	Large organisations	EC_2003 large >250 employees
			Large companies, government and NGOs
			Time and resources for large complex IT systems
			Likely to have developed policies
			Likely to have multiple layers of security measures
			Government only differ with occasional higher level of perceived risk and the level of accountability in procurement process
			Government = risk owner for UK Plc so the economic risk of widespread attacks
		Individuals connected to large stakeholder	*Cross-pollination of cyber security knowledge from workplace*
Digital Footprint			*Impact on culture of an inability to forget past actions and move on*
			The intersection of privacy and small-scale cyber security
			1. Definitions of privacy for the individual
			a. Intersection with identity/reputation
			b. Value of data to the individual
			c. Discussion on whether the privacy of an organisation exists, or is simply security?
			2. Definitions of security for the individual
			a. Intersection with identity/reputation and differences to point 1.a
			b. Value of data to third parties -- adversaries or others as part of a transaction
			3. Links between confidentiality and privacy changes in value proposition of data over time... value of data to individual as part of ID/reputation changing as the environment changes (employment/social group etc./cultural \& societal changes)
			4. Implications if the individual's cyber footprint is linked to the company's footprint
			5. Other stuff in the system

Digital Footprint contd.		*a. ?? similarities -- degradation in privacy/security over time as environment changes? Data protection only involves the living, in the context of data release "causing harm to the individual" -- implications of data release on family etc.*
		b. Play-off cyber security models which reduce privacy for the sake of safety
		c. Vulnerable users -- intersection with safety/physical security
		Look up reasons for seeking privacy (Goodwin 2002)
		Is privacy a social contract -- collectively collude to create an illusion? Source of privacy as a concept?
		Social contract theory...
		Dehumanisation of people when considering "big data"
		online identity is a composite of different roles. Overlap into the real world, the power of information online and the level of credibility given to information online (false information on forums/Wikipedia vs old information sources)
		Association (and brand association)
		The risks associated in linking different identities
Time	Time	*Changing value of data in changing environment*
		Question of future security risk for data released
		Security of the individual different to privacy
Security vs Privacy		*Security not necessarily treated in service contracts - often only in terms of privacy/data protection*
		Privacy treated in law
		Ability of the quality of service legislation to cover security
		security by using a single supplier for multiple services compromises privacy
		even paid-for services compromise privacy - level of data transaction not part of the 'enhanced service'
		lack of consumer control/power over pre-existing data
		implicit choice/consent
	Security of the Individual	*Security in its broader sense - financial stability etc.*
		security depends on ownership and the variety of services used - the number of agents to rely on and surface area of footprint
		security of preserving privacy where limiting use not possible - extension of data protection
		cultural security - the expectation/right to be forgotten and learn from mistakes
		integrity of data in cyber footprint
		MP2 reliance on cyber footprint to advertise company
	Privacy Measures	*adapted social media use to enhance privacy*
		dehumanisation of individuals as subjects in big data
		need to limit or fragment web service use to preserve privacy
		privacy by pragmatism
		cost-benefit analysis
		attempt to avoid linking accounts
		actors in small organisations share more personally identifying information online
		cyber footprint is a composite of roles
		practice of organisational distancing from forums etc. - unofficial official
		SSITU\16 browser cookie blocking
		SSITU\16 no use of browser add-ons: questionable credibility
		SSITU\16 limited web surfing to reduce tracking
		SSITU\16 pragmatism cost-benefit analysis limitation of use/sharing to retain privacy
		SSITU\16 cabled home network to avoid eavesdropping
		SSITU\16 choice of services that don't collect data - why 'pay' for uninteresting distractions with data, ad-free services as preference
		SSITU\16 avoidance of linking accounts. Attempt to control data aggregation through use of multiple credentials.
		SSITU\16 data protection awareness and behavioural changes to protect privacy of others (customers) in home network
		SSITU\16 choice not to use free apps whose purpose is marketing rather than service
		MP1 privacy legislation conflicts with typical focus of safety on availability

		Privacy Measures contd.	ICO_actions ICO case stories which could offer advice all written to advise consumers about data use/accuracy (DPA/FOI), without cyber breach examples or examples to organisations on how to apply data protection law
			ICO_actions undertakings - failure of procedure/security or lost equipment with no negative outcome on data users... includes a follow up to check improvements have been made
	Cyber footprint		*lack control of transference of data from 'public' to 'cyber-public' domains*
			large scale services creating 'public' datasets (e.g.. Google Maps)
			data aggregation
			lack control of associate-created data
			small organisations need a cyber presence
			cyber footprints of small organisations confounded with the personal footprints of their actors
			attribution of social presence to organisation
			limiting cyber footprint is limiting internet use or interconnections
		Public Data	SP\15 systematically shared data - phonebook etc. more easily available facilitating social engineering
			SP\15 data which can't be controlled (e.g.. google streetview) make it easier for attackers to socially engineer local businesses
		Right to be Forgotten	SSITU\16 people deserve forgiveness if they have changed and moved on
		Social Media	SSITU\16 adapted use, omitting details, can increase privacy
			SSITU\16 privacy settings used to keep accounts closed
			SSITU\16 publicised lapses in judgement - what to share, understanding the magnitude of the audience shared with
			SSITU\16 vulnerable to poor decision making in social media use - potentially career destroying
			SSITU\16 unintentional disclosures on Twitter have a level of permanence damaging ability to be forgotten
			SSITU\16 written content on social media has to be interpreted more strictly than spoken word leading to harsher judgment
			SSITU.SP\19 recommends social media training for charities/clubs to avoid unintentional disclosure
			SSITU.SP\19 club made the choice not to create a forum to avoid the responsibility for policing trolling
			SSITU.SP\19 member-led club forums on 3rd party services, moderated by volunteers but without the club having sufficient control to ensure that there is always a member administrating
			ACCTS_guide_2015 widespread use of social media is leaking/spreading news of compromise increasingly quickly
		Footprint consequences	*social media makes people vulnerable to public poor decision making*
			the written word leads to harsher interpretation/judgement
			social media speeds up the diffusion of news - breaches
			the smaller the organisation the easier they are to target
			the ability to move on given data-permanence
			requests to the ICO for 3rd parties to enhance the integrity of their data to reduce harm - decoupling ex-spouses' credit scores etc.
			delays in updating data / incorrect assumptions
			cyber security risk of linking roles
			magnitude of impact related to level of interconnections (LIT???)
			risk in people giving credibility to information found online
			risk of trolling
			risk of reputational damage
			difficulty administrating social interactions on 3rd party services
Cyber Decision Making			*impact of service reliance in decision making*
			outsourcing - transfer of cost to user as risk/privacy reduction
			the increase in value of data once customers are strongly identified
			questionable that the majority of consumers realise that their data is an asset
			does the ability to see cyber threats imply responsibility
			influence of security measures on sale price - case study 14?
			increase in risk once extra data held as asset
			making secure decisions when it's free and easy

Ultimate goal of training to increase incentive: ``I can do this easily at an affordable cost, and everyone else is doing it so it must be due diligence'' ??

Other small organisations will differ in that their decision making processes will be dependent on their mission, which may alter their attitude to decision making. \graffito{I'm sure I've already read some stuff to cite here...} Home users will differ in comparison to single person companies in that they are unlikely to want to adhere to standards. Measuring personal security will be different to that of a brand image or company reputation.

Cyber security products are subject to fashion as much as any other sector. This may have more impact in the small-scale sector than in large organisations (number of people involved in decision making, speed of decision making, lifetime of decision implemented) influence of fashion on standard practice cyber security in the home by the experts due diligence
blind mitigation -- the application of measures without understanding risk can transform risk and damage socio-technical aspects of an organisation.

vulnerable users - BBC safety survey / get safe release. Implications of pervasive Wi-Fi on content filtering models. GLOC POL student report
would implementing uniquely a monitoring system and good behavioural training have more impact than other non-default measures
data subjects made vulnerable by a lack of control of their data
data subjects might need decision about 'illegal' data leak to defend themselves/be able to move but ICO waits to see impact on subjects before making judgment

Privacy

"already a veneer"
assumption of no privacy in decision making
nothing to hide = security decision not privacy decision
need a measure of the sensitivity of data to make proportionate decisions about security/privacy
ICO interventions consider impact on data subject
measure of sensitivity - risk of user distress, harm, ill-health or critical service discontinuity
Privacy erosion
- *responsibility to users/organisation to provide security*
- *blocks/erosion privacy to increase data asset value*
- *privacy blocks more obvious in mobile sector*
- *surveillance easer than guarding privacy - question of proportionality*

privacy-conscious decision making impacts cyber footprint
SSITU\4 assumption of no privacy
SSITU\16 societal attitude of "nothing to hide" degrades when faced with a decision about personal privacy.
SSITU\16 when faced with a decision about reducing privacy differentiate people can on a need to know basis
SSITU\16 privacy is a veneer given physical surveillance (CCTV) and the risk of data aggregation

Privacy Erosion

SSITU\14 balancing responsibility to provide secure services and privacy in the internet supply chain
SSITU\14 the need to monitor for security contentious with employees
SSITU\16 jurisdictional/risk issues of outsourcing overseas, especially for vulnerable users (e.g.. NHS)
SSITU\16 blocks to privacy measures - Apple forcing users to supply credit card details for the app store despite the ability to use the service for free.

SSITU\16 mobile apps request too many permissions
SSITU\16 IoT implementation requires sufficient security to protect privacy

Surveillance

SSITU\16 data aggregation is easy but requires justification
SSITU\16 disproportionate and with questionable legality - reactionary decision making given increased influence of the news. Unjustified in times of higher risk - IRA

Vulnerable Users

vulnerable users different to user vulnerability
- *Children and teenagers*
- *child - monitor use*
- *no filtering applied*
- *filtering possible*
- *education and trust most important*
- *7 too young to need educating about content*
- *teenagers get some supervision*

Vulnerable Users contd.		*Other vulnerable users*
		Don't have to use IT to have a footprint to protect
		User/organisational vulnerability
		evolution in law enforcement: perception of 'victims' of crime, increased sympathy, even where victim used to attack others
		system and service dependence can introduce user vulnerability
		social media profiles retained despite abuse - "take a break" rather than delete
		any user could be vulnerable in given context of breached data
		cyber footprint integration of questionable legality
		need for cyber presence increases vulnerability
		protecting an organisation may make its users more vulnerable - distancing from official-unofficial social media profiles to avoid moderation requirement
	Children	SSITU\3 monitored use
		SSITU\3 security measures (filtering) not activated
		SSITU\3 7 years old - too young to need education about content
	Teenagers	SSITU\1 education and trust
		SSITU\1 filtering technically possible but not implemented
		SSITU\17 supervision, no access control or filtering
	Any users	SP\12 law enforcement: those hosting malicious content after attacks are victims not criminals
		SSITU\16 service dependence - social media - forcing abuse victims to retain public profile
		ICO_2 ICO considered users to be more likely to be distressed due to context - BPAS/medical AND motivation of attacker to do harm/cause distress to the organisation and its customers
		ICO_2 ICO measures emotional distress as an outcome of a breach even where leaked data did not do harm
		ICO_3 this contravention posed a significant risk of causing serious detriment to thousands of prisoners
		the data subjects would be likely to suffer from substantial distress knowing that their confidential and sensitive personal data may be accessed by unauthorised third parties
		If the data has in fact been accessed by untrustworthy third parties then it is likely that the contravention would cause further distress and substantial damage to the data subjects such as exposing them to physical harm.
		ICO_4 the loss of the sensitive personal data is likely to lead to the ill-health of those affected through the disclosure of the data or due to a break in the services which they were receiving A small number of reports identify the parents of a pupil, and contain information about the "home-life", which includes financial matters and family dynamics. The data subjects were not notified of the data breach. damage and distress to the data subjects is substantial due to the volume of data which has been lost
Security Decision Making		*reliance-influenced decision making*
		'more secure' cloud not free - data transaction
		lack of knowledge of value of data assets
		does visibility = responsibility?
		risk increased by data assets
		good security implemented when free and easy
		indiscriminate security: product fashions; blind mitigation can damage socio-technical processes
		vulnerability from lack of personal data control
	Password management	*difficult*
		CE mandate hard to achieve
		main means of securing many IT functions
		choice of device - using trusted platforms - perceived security
		retrieval/memory techniques
		soft/hard copies
		bi-monthly calendar reminders
		evaluate credential value
		reuse
		SSITU\4 systematic password creation to aid memory

Password management ctd.	SSITU\4 multiple soft and hard copies of passwords
	SSITU\4 renewed every 60 days with reminder
	SSITU\5 small orgs have problems keeping up to date with changes
	SSITU\5 Cyber Essentials mandate hard to achieve
	SSITU.SP\8 cloud may offer interesting solutions to password management
	SSITU\17 main means of security - all accounts have password
	SSITU\17 non-valued accounts reuse the same password
	SSITU\17 valuable credentials get stronger and unique password
	SSITU\17 use laptop instead of phone for online purchases - harder to steal when holds credentials
Attitude to security	*some orgs commitment questionable*
	reputation is everything
	trust at face value - no red tape
	standard security sufficient
	disconnect security and revenue growth
	unlikely to employ consultancy
	SP\9SEC insights to security behaviours:
	love the web;
	digital infants;
	not on my radar;
	not a hacking target;
	faster, better, connected;
	online autopilot;
	unreal digital actions;
	who is in charge?;
	poor decision making on mobile devices;
	too complex and time consuming
	people want to look competent
	Specific to SMEs:
	web designer tells me what I need - unlikely to use an IT consultant
	reputation is everything - keeping data and customers safe is vital
	trust is at face value - avoidance of red tape and burocracy
	standard security is enough - SMEs don't connect security measures with their key concern of growing revenue
	ICO_1 ICO questions commitment to secure data
Free	*requires configuration*
	pay for usability
	free rather than knowledgeable advice sought
	simple techniques/free software significantly reduces risk
	advice available from govt
	no one should pay to be victim
	support for reverse engineering
	SSITU\1 free products require knowledge for effective use
	SSITU\5 free IT support expected despite service provider lacking knowledge
	SSITU.SP\8 micro organisations expect free IT support
	SP\9 advice training from government online
	SP\12 no-one should have to pay for being a victim of crime
	RH.SP\13 free support analysing malware samples for orgs lacking knowledge
	SP\9SEC free software can prevent many attacks
	SP\9SEC simple techniques can reduce risk

Evolution

digital natives - confidence - DIY
larger IT supplier search larger clients - cost efficient
individuals withdrawn support - high maintenance and risk - too high a proportion of cyber footprint shared
IT support replaced by cloud services
reducing customer base for IT support in smallest orgs
increased reliance on IT systems
increased knowledge sharing partnerships
encouraging security as a service in product/service suppliers
service dependence - reticence to drop services after changes
safety standards evolution need to catch up with cyber risk
digital natives - higher service expectations (inc of employer)
need to retain safe/secure unconnected devices
IT-Driven evolution product to service
difficulty translating technical to business risk
implications of cyber decision making
improvement on carrying out the basics
attitude of breach inevitability
need for plan
focus on critical assets
cloud supplier rhetoric: evolution towards cloud; unavoidable/inevitably becoming the way business is done; influence of increased mobile use; efficiency and agility benefits; cloud adoption by IT exception sprawl
lack of appropriate skills
difficulty managing complexity
more training being given
cyber getting less tech, more mainstream
SSITU.SP\8 digital natives do DIY IT
SSITU.SP\8 adapting to threats can't cause business disruption
SSITU.SP\8 size of customers has grown with the size of the company
SSITU.SP\8 reducing the number of individuals as customers - high service level required, vetting of employees and risk of high profile individuals
SSITU.SP\8 micro companies are swapping IT support for cloud reducing the client base
SP\10 increased reliance on IT systems
SP\12 partnerships help to improve knowledge of how to make security products appealing
SP\15 encouraging security as a service as a business opportunity rather than an onerous task
SSITU\16 changes in service haven't led to dropping a service - careful/suspicious when choosing so no problems yet... service dependence?
SSITU\16 suspicious of the evolution of services when increased data collection involved
SP\18 safety standards evolve to catch up with risks
SSITU.SP\19 service requirements increasing with increase in digital natives
MP1 inclusion of networked capability leads to new responsibilities/business drivers for both customer and suppliers
MP1 evolution of business drivers
Netskope_guide_2015 - use of cloud SaaS model
  Rhetoric of a cloud supplier
  increased cloud use for ease/efficiency
  slow adoption is because businesses are "intimidated" by the use of cloud
  there is a growth of business use of the cloud
  growth is influenced by increased mobile use
  companies "should" integrate cloud into daily business
  cloud is inevitable - "the way business is done"
  IT activities of entire functional groups are moving into the cloud

Evolution contd.	cloud provides agility, device choice, facilitates collaboration, at minimal expense
	organisations should "safely enable" the inevitable
	the growth of cloud app use is by IT "exception sprawl"
	use of thousands of apps across almost every function
	ACCTS_guide_2015 orgs are struggling to translate cyber risk from technical to business
	ACCTS_guide_2015 increased acceptance of inevitable breaches and the need for rapid response to incidents
	ACCTS_guide_2015 little evidence has emerged of the impact of information sharing
	ACCTS_guide_2015 increased focus on critical assets
	ACCTS_guide_2015 getting the basics right is the greatest area of improvement in large orgs over the last 2 years
	ACCTS_guide_2015 key challenges such as complexity and obtaining the appropriate skills are still an issue
Good Practice	*pragmatism and proportionality*
	gp = benchmark
	training to highlight good behaviour
	web developers lack incentive for gp
	contracts without support should be poor practice
	IT support assesses customer risk as own
	gp indicator = speed of reaction to compromise
	security is good housekeeping (embedded proc
	prevent breach or success
	gp different in small org - overview possible
	proactively look for incidents
	small orgs share roles to get breadth of knowledge
	knowledgeable developer may refuse contracts with customisation for reputational risk
	small - gp is independently achievable
	understanding cross-disciplinary risk
	SP\2 pragmatism and need rather than attempting absolute security
	SP\7 companies build to be sold by venture capitalists are more careful to follow good practice
	SSITU.SP\8 web developers often display poor practice - contracts without support, platform customisation
	SSITU.SP\8 good practice - updates - may be punished if poor suppliers were employed beforehand
	SSITU\8 IT support - assess customer risk as an extension of own risk
	SP\10 making cyber/info security part of general good housekeeping
	RH\11 training and incentives for suppliers to highlight expected behaviour
	SP\12 time to react to a compromise and the need law enforcement have to contact an org can be an indicator of good practice
	SSITU\14 prevent: incident or prevent incident success; timely detection of inevitable attacks; backup trusted copies of logs for investigation
	SSITU\14 good practice in small orgs is not scalable due to the need to have an overview
	SSITU\14 blending the IT/security in smaller orgs to get a broader skill spectrum and system overview
	SSITU\14 proactive security - incident hunting and investigation by human beings - technical measures don't take decisions
	SSITU.SP\19 layered measures, backups, ability to recover quickly even when required to scrap an element of the system
	SSITU.SP\19 refusing contracts which include CMS customisation
	MP2 the SME study showed that (contrary to concern) SMEs are attempting to make decisions about cyber security based on an evaluation of their current cyber capability
Safety Good Practice	*MP1 for definitions and evaluation of current state of affairs*
	safety gp well established
	bridge to consumer cps underdeveloped
	understanding complexity
	ownership
	software treated only as static element in safety gp
	cps lifespan

Knowledge

self-reliance a facet of entrepreneurship
complacency risk - no knowledge
knowledge as a self-efficacy destabiliser
easier to assess risk in a home environment
education harder than implementing tech
training has to be updated with policies
narrow window for cyber maturity building
small orgs educated as consumers not business
knowledge of emerging system - understanding where to put security in ccps
questionable awareness
how are attacks found
resource to find attacks
rising non technical awareness
understanding how to act/react a challenge
knowledge of service contract consequences
risk prioritisation issues
cyber fashion and fatigue - lifespan of awareness
ability to remediate
training reduces security work-arounds
size changes level of remediation support required
lack understanding of website maintenance
lack of resilience in staffing for security
availability of volunteer experts
compliance - cyber risk becoming audit issue
non-tech execs required to be come tech savvy
knowledge of consequences for getting it wrong - arrest for bad data
knowledge of what data has value
lack knowledge to ask questions about system function
ICO require understanding/demonstration of cyber gp and risk
SSITU\1 questionable availability of expert knowledge
SSITU.SP\5 SMEs lack security awareness
SSITU.SP\8 customers don't understand the implication of contracts without support
SP\9 in education small organisations are treated as typical consumers
SP\9 small orgs unsure how to handle cyber issue
SP\10 rise in awareness in recent past
SP\10 many small orgs aware but unsure how to act
SP\10 knowledge in a non-technical sector improving
SP\10 aware but don't know which risk to prioritise
SP\10 lifespan awareness given likelihood of fashion to be followed by fatigue
RH\11 awareness training reduces security work-arounds
RH\11 don't know where to put security in emerging IoT systems to reduce vulnerabilities
SP\12 the size of an ISP influences knowledge and so the level of support they need to remediate
RH.SP\13 government point of contact for support with forensic analysis
SSITU\14 questions awareness of all attacks which could have happened in the network
SP\15 small organisations have questionable ability to remediate after an attack
SP\15 small orgs might not have the resource to find or manage threats
SSITU\16 consumers confused with the quantity of security products
SSITU\17 user lacking security product awareness and using default settings
SP\18 user expectation products need no knowledge/maintenance to be safe

Knowledge contd.	SSITU.SP\19 committee led organisations lack knowledge of what they need
	SSITU.SP\19 customers don't understand the time investment needed to run a website
	SSITU.SP\19 charities/clubs could have low availability of volunteers with appropriate technical skills or non tech-literate volunteers are chosen for non-technical skills
	SSITU.SP\19 cyber awareness prompted by the arrest of a friend who was victim of a cyber crime - high risk of getting it wrong
	SSITU.SP\19 IT support has no resilience plan to cover illness, can only use standard software and hope charities find someone if needed
	SSITU.SP\19 volunteers make mistakes and charities lack policies to protect privacy
	ACCTS_guide_2015 increase in cyber risk awareness - source: personal experience, media, UK government initiatives (FTSE 350 tracker)
	ACCTS_guide_2015 auditors are asking more questions about how cyber risk is managed
	ACCTS_guide_2015 increased awareness has led to greater resources
	ACCTS_guide_2015 more non-technical board members are beginning to gain confidence and question the information they are bought by CIOs
	ACCTS_guide_2015 improving behaviour is critical in improving cyber security
	ACCTS_guide_2013 small business owners likely to be surprised about what data has a value
	ACCTS_guide_2013 companies need to work out how they know there is a problem
	ICO_2 BPAS understanding of the function of their website was different to that which was implemented due to changes in functionality to de-risk data held... risk analysis decisions obfuscated rather than reduced risk due to lack of knowledge
	ICO_3 NOMS didn't understand that encryption software needed manual activation so did not instruct their supplier to do it
	ICO_3 "The data controller holds responsibility within Government for Government policy on data protection matters and could therefore be expected to be a model of best practice and exemplary in respect of data protection compliance"
	ICO_8 the Commissioner determined that the data controller had not displayed an understanding of good security practice, nor the real risk presented by an internet-based attack.
	MP2 link between knowledge and confidence - inverse proportion
	MP2 intimidated by perceived risk
	MP2 burden of knowledge required by one person to understand security
Training	RH\11 training focused on home to help employees visualise risk
	SSITU\16 education about password management etc. harder than implementing network security
	SSITU.SP\19 charity volunteers do website content management - tech skills harder to train than media training
	SP\20 law enforcement initial responders trained to give cyber prevent advice
	ACCTS_guide_2015 increased amounts of training being given in companies, but further investment may be needed to make improvements sustainable
	ACCTS_guide_2015 cyber training moving out of the IT function and into more mainstream functions helping to embed cyber into daily practices
	ACCTS_guide_2015 lack of engagement from subject matter experts in training who could provide understanding of the real-life application of security measures
	ICO_4 encrypting removable media was in the new security policy, rolled out 4 months before the policy was part of a pre-login disclaimer which employees had to agree to before logging into a system training was via e-learning and not mandatory before the incident. The teacher had had security but possibly not DPA training The data controller obtained confirmation from the teacher in June 2011, that they had read and understood the new information security policy.
Security Measures	*experts can configure home n/w with security in mind*
	product security drivers: pragmatism, adequacy (reputation and flexibility), proactivity, competitive edge
	secure product defaults assume novice users
	indiscriminate security a concern
	assume network insecure
	secure choice not windows
	availability over confidentiality
	resilience over security
	security fatigue
	questionable product efficacy
	choice not to worry - security equivalent to everyone else

Security Measures contd.	*unexpectedly poor policies in small orgs*
	rigorous policies
	permissive policies to prevent circumvention
	internal monitoring of outsourced services to "keep them honest"
	security a barrier to tech use
	inaction on 'free' security - policies (indicating lack of knowledge)
	need to discover cyber footprint
	notion of "enterprise ready" software/apps
	potential underestimation of cloud use
	need reactive security budget for unknown unknowns
	security overkill in an attempt at future-proofing
	limit/partition service use to retain control of privacy and security
	employer IT choices limit home user control
	pragmatism/adequate security
	balance - practical security and appropriate privacy
	computers preferred for higher-risk activities
	credential protection by manual entry
	measures don't make decisions people do
	proactive monitoring limits employee freedom in very small organisations
	choice not to use insecure option when equally prices secure option available
	velocity of information (bad news) requires proactive approach
	3G seen as more secure than free Wi-Fi
	inherent security
	security by afterthought
	security maturity
	organisational need for profit
	avoid indiscriminate security
	number and choice of services - cyber footprint
	SSITU\1 control of the home network
	SSITU\1 incident response strategy a factor in home network configuration
	SP\2 pragmatism - business requirements and security
	SP\2 security measures aim to provide "adequate protection"
	SP\2 preference for proactive security - cost efficient
	SP\2 budget for reactive security to deal with unknown unknowns
	SP\2 limiting security measures developed to retain competitive edge
	SP\2 security measure configuration assumes novice users
	SSITU\3 concerned about indiscriminate security
	SSITU\3 knows network is insecure
	SSITU\3 not windows
	SSITU\3 availability over confidentiality
	SSITU\3 questionable efficacy of security products
	SSITU\3 resilience over security
	SSITU\3 security fatigue
	SSITU\4 availability over confidentiality
	SSITU\4 pragmatism
	SSITU\4 resilience
	SSITU\4 choice not to worry
	SSITU\4 indiscriminate security would be a barrier to technology use
	SP\5 customers in network have unexpectedly low security - no backups or separate admin accounts

	Security Measures contd.	SSITU\8 rigorous policies, keeping only the data the company needs to hold
		SSITU\8 resilience, layered backups
		RH\11 supply of high-quality equipment and permissive policies to encourage use without security circumvention
		RH\11 internal monitoring required to keep IT service provider honest
		SP\12 pragmatism in law enforcement to differentiate victims from cyber criminals
		SSITU\14 security overkill hopefully sufficient to cover evolution in threat profiles without major adaptations
		SSITU\16 minimal mobile apps used due to permissions required
		SSITU\16 attempt to make unintentional disclosure by data aggregation hard by avoiding linking accounts
		SSITU\16 employer choices of platforms used for home working limit control and privacy
		SSITU\16 pragmatism/adequate protection
		SSITU\16 default to privacy, making choices by limitation of IT use
		SSITU\16 balancing practical security and appropriate privacy
		SSITU\17 valuable credentials entered manually each time - not stored
		SSITU\17 online purchases/higher risk transactions carried out on a laptop rather than a phone
		SSITU\17 3G is more secure than free WiFi but will still use free network if free minutes finished
		SSITU.SP\19 proactive monitoring of system is pragmatic but not ideal - lack freedom. Less than 1 concern per year
		Netskope_guide_2015 - use of cloud SaaS model
		steps - discovery, app use, risk assessment, policy development, monitoring and compliance enforcement
		even apps sanctioned by IT may not be enterprise ready
		most enterprises underestimate their cloud use by 90%
		ACCTS_guide_2015 the speed of the spread of bad news makes proactive security measures more important
		ACCTS_guide_2015 advise that security become an inherent property rather than an afterthought
		ACCTS_guide_2013 avoid deploying limiting security measures out of fear (indiscriminate security) because companies need to profit form the online world
Business Decision Making	Trust	*home working - trust other n/w users? implicit trust*
		trust free unqualified network provider
		too much trust in suppliers from individuals
		expect safe/secure network
		different security reqts for trusted suppliers
		trust insecure network rather than staying offline
		expectation of connectivity
		lack abundance forces trust - complacency
		lack trust in sec security measures - snake oil sales, vulnerability of unknowledgeable users
		lack of partnership/interaction seen as inaction, reducing trust - independence
		SSITU\1 limited trust of own family in home network - corporate-style controls employed
		SP\5 SMEs trust an unqualified network provider without question
		SSITU.SP\8 individuals place too much trust/access in their IT suppliers
		SSITU\17 user expectation that network suppliers provide safety and security in both work BYOD network and home ISP provided network
		SSITU\17 makes exceptions in self-imposed security measures for trusted suppliers
		SSITU\17 service dependence/pragmatism in choice of network - will use less secure networks if that's all available
		MP2 concerns about security awareness not the realisty in SMEs - other constraints
		MP1 expecation of plug-and-play safety without education
	Cost-Benefit Analysis	*proactive vs reactive security*
		compliance - no interest in govt market for other time delay reasons
		limited government resource - contact as many as possible about cyber security
		IT dependence outweighs risks
		need vs privacy

Cost-Benefit Analysis contd.	*risks and selling point - remote control CPS*
	speed of growth in outsourcing decisions
	cloud offers flexibility
	cashflow risks vs cyber risk
	resource constraints
	disparity - large orgs own sec vs sec supplied to consumers - "eat your on dog food"
	bad response amplifies problem
	contract lockins reduce security supplied
	"good incident response" = good communication
	bad communication amplifies impact
	response strategy required
	easy fast and cheap given more attention than important
	SP\2 balance of resource allocation for proactive or reactive security measures
	SP\7 immature companies don't aim at government marketplace sue to the time/resource required to secure a contract
	SP\12 need to use limited resource to contact as many victims as possible
	SP\12 law enforcement takedowns are dictated by prevalence
	SP\15 need to be online and service dependencies often outweigh knowledge and risk awareness
	SSITU\16 balancing the risk of over-sharing against the value of an online presence
	SSITU\16 balancing a need for a service against privacy
	SP\18 remote access is a key selling point in IoT but also introduces safety risks
	MP2 IT choice based on company growth and finances
	MP2 cash flow dicatates choice of CAPEX/OPEX
	MP2 SMES have very limited resources to invest
	MP1 limited obligation to provide security as a service to customers
	ACCTS_guide_2015 having a response strategy in place in increasingly important to placate customers
	ACCTS_guide_2015 "good response" = speed and openness, contacting customers rapidly to provide breach details and advice
	ACCTS_guide_2015 "bad response" amplification of breach impact by slow response and poor communication
	ACCTS_guide_2015 finite resources need to be focussed in the right direction
	ACCTS_guide_2015 businesses tend to focus on the easy/cheap measures rather than the most important ones
	ACCTS_guide_2013 the digital economy relies on digital technology to function
Assets	*low value assets - reason for low security*
	value in business process different to data
	unpatentable/post patent = low risk/value
	ID value - improve security efficiency
	credentials - alter behaviour on value
	SSITU\3 considers all digital assets held as low value
	SSITU\4 value of assets contributory to security decisions
	SSITU\4 low risk assets - IP is copyright not patentable
	SSITU\4 business processes are a higher value asset than documents held
	SP\7 assets - IP - low risk in post-patent startups
	SP\10 members define diamonds in the data assets to make security more efficient
	SSITU\17 definition of valuable credentials and altered behaviour
	ACCTS_guide_2015 there is a growing requirement in large organisations to classify data so that key assets can be protected
Resource	*customisation magnifies security issues by delaying patches*
	day to day tome constraints
	financial constraints limit decision making
	reasonable time to deploy
	size of IT reqt limits security opportunities - leads to shared hosting

Resource contd.	*sec products expensive because of subscriptions*
	marketplace - appeal of low resource sector to suppliers
	small = lack of economies of scale
	effort of support > building so not offered
	resource limits number of notifications
	low knowledge - lack of affordability
	cost of security in products is lack of flexibility
	cost of products include security
	compliance - motivate SMEs to dedicate adequate resource - indivisible risk and incentives
	CE compliance depends on level of investment
	free access to process for CE - can use to influence ongoing process
	SSITU\1 financial constraints in decision making
	SP\2 financial constraints in decision making
	SP\2 development time needs to be reasonable
	SSITU\3 the time security measures take to deploy is an issue
	SSITU\5 size of requirement and resource limits choice - most small orgs don't need a whole server
	SP\7 startups only spend 8 months in incubator - too short a time to worry about security
	SSITU.SP\8 customisation delayed patching magnifying an issue by allowing an incident
	SSITU.SP\8 takes more effort to support a site than build it so web developers focus on highest returns
	SSITU.SP\8 security products expensive - 1 off cost and subscription
	SP\9 small orgs and individuals have a small budget
	SP\10 financial, time and knowledge constraints in decision making for small orgs
	SP\10 day to day time constraints in small orgs make cyber harder
	SP\15 the proportion of victims notified depends on the prevalence of attacks in a certain region
	MP2 perceived affordability is based on problem owner's research - expect unaffordable
	MP2 extreme financial constraint in line with size and availability of economies of scale
	SP\9SEC different options depending on investment - free download of process; paid for certification of self-assessment; certification of systems in situ using penetration testing
Need	*threat intel and success metrics*
	evolution in tech should augment performance
	consistency between platforms
	cost benefit and pragmatism vs privacy
	SSITU.SP\8 cyber threat intelligence
	RH\11 ability to provide consistency over different platforms for BYOD
	SP\18 IoT products should be about augmented performance
	SP\19 need to hold too much data for legacy processes in some charities/clubs
	ACCTS_guide_2015 businesses need to change their mindset around security
	ACCTS_guide_2015 good management of cyber risk hindered by a lack of metrics for success or breach impacts
Business Processes	*securing reputation, goodwill*
	reluctance to update incumbent processes
	startup process avoidance or immaturity
	sectoral view - risk averse/audit-involved = more receptive to security
	budgets for routine threats
	assume continuous compromise
	lack business process for detection and response
	lack of infra to adopt safety gp
	embarrassing minor attacks as motivator
	positive behavioural adjustments
	cyber incentives

	Business Processes contd.	*reactionary policies disproportionately damage privacy*
		outsourcing defined before cyber - outdated contracts
		simplicity - single enterprise system
		volume of cleanups increased when ISPs notify
		testing cyber business processes can ID supply chain issues
		small have different problems
		mobile devices needed for travel
		charities/clubs lack leadership stability
		charities/clubs rely on volunteers special interests for decisions
		SSITU.SP\5 security improved to protect reputation
		SP\7 long-term growth organisations see no need to radically change business processes to improve security
		SP\7 startups have immature business processes
		SP\10 risk averse sectors receptive and better at security
		SP\10 cyber is becoming a routine threat - breaches expected and budgeted for in smaller orgs
		SP\10 discussion about cyber threats needs to begin at board level
		SP\10 some organisations assume a continuous state of compromise
		SP\10 small organisations lack the business processes for cyber incident detection or response
		SP\10 sectors where the audit role is familiar have increased receptiveness to cyber security measures
		RH\11 employees more effectively learn secure behaviour in the home environment
		RH\11 IT outsourcing defined/contracted before security became a major issue
		RH\11 need the simplicity of a single enterprise system
		SP\12 engagement of ISP in attack notifications increases the volume of cleanups
		RH.SP\13 exercises to test cyber business processes can help identify weaknesses in supply chain
		SSITU\14 embarrassing minor attack in distant past a motivator for current secure practices
		SP\15 large orgs have different cyber issues to small ones
		SP\15 minor security reaches can provide positive behavioural adjustments
		SSITU\16 reactionary changes in business processes after a safety/security incident can cause unnecessary privacy erosion
		SSITU\17 mobile devices used during travel
		SSITU.SP\19 charities/clubs can lack stability in leadership - committees can break down. Heavy reliance on IT peer-support for business continuity
		SSITU.SP\19 charity/club cyber footprints reliant on the special interests of committee members, knowledge and confidence, rather than need
		SP\20 development of cyber crime prevention methods based on those for other business crime (theft/burglary)
		MP1 development team evolving, becoming more complex, unclear responsibilities
Usability	Usable decisions	*combat lack of knowledge by using single supplier*
		usable cyber sec different to usable IT - understanding consequences
		services make privacy/confidentiality by default difficult
		cyber-accessibility dependent on knowledge
		SSITU\1 single supplier
		SSITU\1 questionable knowledge makes secure solutions inaccessible
		SP\2 in cyber security means that users comprehend the consequences of their actions
		SSITU\16 many integrated services (e.g. cloud backup from mobile manufacturers) make defaulting to privacy hard
		Netskope_guide_2015 - use of cloud SaaS model
		efficiency for employees, get job done quickly and with flexibility
		minimal effort to get running
		ease of use leads to "Shadow IT" where apps are used without organisation's knowledge
		security measures like CASB should 'coach' users to make good choices
		cloud vendors should provide granular information about app activities for user orgs to build CASB policies
		user org IT dept. should evaluate every app discovered

		Usable decisions contd.	security needs to be transparent and unobstuctive to users to avoid circumvention
Security Incentives	Insurance	Conditions of insurance	*availability of insurance used as an incentive*
			insurance used as a risk mitigation strategy
			insurance requirement replacing security requirement
			patchy cover provided by insurance policies
			insurance tied to compliance
			lack intelligence to develop reliable insurance products
			standards can be used a benchmark to help develop the cyber insurance market
			concerns about the scope of insurance coverage where companies non-compliant or make a mistake
			SSITU\4 gaps in insurance policies for malicious threat causing business interruption
			SSITU.SP\8 incentive to obtain cyber essentials
			SP\9 automatic insurance after security compliance sued as an incentive
		Conditions of insurance ctd.	SP\10 can't cover reputational damage
			SP\10 potentially an incentive against good practice
			SP\10 good carrot for compliance
			Standards_2015 Certain suppliers of cyber security insurance have sold it on the condition that a company comply with Cyber Essentials.
			ACCTS_guide_2015 higher on the agenda as a risk mitigation strategy
			ACCTS_guide_2015 industry hindered by lack of breach intelligence and a lack of clear standards from which to specify required behaviours
			ACCTS_guide_2015 hope that cyber essentials will be the clear standard required to develop insurance market in the UK
			ACCTS_guide_2015 there are concerns about coverage if one of the core hygiene standards are not being followed (or someone makes a mistake)
			strategy requires metrics for success to show initiatives impact
	Support for Small Orgs		*stimulate market growth*
			client base for knowledgeable support to SMEs shrinking
			security knowledge could be used as a differentiator/unique selling point
		UK Cyber Strategy	SP\9 user types for success metrics and tangible goals
			SP\9 stimulate growth in cyber security marketplace
			SP\9 impact of poor security and cyber crime on national economy
			SP\12 metrics providing targets for success
		IT Support	SSITU.SP\8 reduced client base - micro orgs - plus a high cost of security training
			SSITU.SP\8 security knowledge as differentiator in reducing client base
		Reporting	*incident reporting platforms available*
			incident reporting provides stats for handling cyber security
			incident reporting required where an organisation is data controller
			motivation to report reduced by underinsurance of risk
			SP\15 small orgs don't comprehensively report incidents
			MP1 lack of reporting makes it unclear how responsibility users are taking for their own mistakes
			ICO requirement for data controllers to notify the ICO that they are holding data and report incidents
			risk avoidance by behaviour modification
	Risk		*free measures at personal cost - freedom of actions online*
			basic measures for risk reduction - cheap/fast/easy
			due diligence (fashion) as an incentive
			threshold of acceptable risk after the basics completed?
			cloud - knowledge/control reducing
			knowing contractual/legal rights as a block to cloud adoption
			can't outsource cyber risk

Risk contd.

risk assessment too high resource
secure virtual organisation - risk retained by customer
lack knowledge of risks
assets protected by legal path - copyright/patent
security requirement equivalent to perceived risk
incubators insulate startups from risk, so from security incentive/knowledge
defence supply chain example of chain facing targeted threats
cyber insurance can't mitigate reputational damage
BYOD gives users a conflict of interest
customers represent risk to suppliers
basics only mitigate commodity threats
small organisations are seen as the weak link in the supply chain
visibility/obscurity still alters risk
attack impacts higher in small organisations
too small to survive/too big to fail
reputation - consumers have a short memory
ICO provides quantifiable risk
ICO rules within the means of an organisation
do you block risky software or specific activities on it?
overview of a small organisation vs large organisations risk analysis
risk of non enterprise-ready cloud services
inherent risk in holding data outside of the organisation
risking the use of free consumer services for business
financial resilience critical in case of breach
good communication critical in surviving a breach
economic impact of undermining consumer confidence
data value measure - willingness to give it away
all data has a value to someone
value is a threat incentive
risk is defined by the value of an information asset to anyone (privacy - sensitivity/value of confidentiality to an individual)
ICO maximum penalty of 0.5M
cyber risk of legacy systems can be equivalent to data / continuity loss
cyber risk needs evaluation in project planning
MP2 evidence of risk avoiding behaviours
SSITU\1 risk retained by customer - employees work from their site with customer machines
SSITU\3 little perceived risk so sufficient security without measures
SSITU\3 security role does not increase risk at home
SSITU\4 no formal risk assessment despite having knowledge
SP\7 risk reduced post-patent so no need for security
SP\7 startups housed inside a big corporate network, not in open internet
SSITU.SP\8 high profile individual present catastrophic risk to their suppliers
SP\9 defence supply chain can't use Cyber Essentials as they have more than commodity threats
SP\10 risk averse industry
SP\10 being risk averse increases the relevance of cyber security
SP\10 cyber insurance can't mitigate reputational damage
RH\11 BYOD introduces a user conflict of interest
RH\11 outsourcing doesn't export risk
RH.SP\13 smaller orgs are the weak link in the supply chain
SSITU\14 visibility alters threat profile

Risk contd.	SP\15 the impact of loss from cyber attack greater in a small organisation
	MP2 data protection fines the only quantifiable risk
	MP2 Small organisations are far less likely than large organisations to do a formal cyber security risk analysis - too heavyweight
	Netskope_guide_2015 - use of cloud SaaS model
	concerns sensitive data
	data leakage
	the majority of apps in use in business are not "enterprise ready" - they lack compliance to standards of security, auditability and business continuity
	there is an inherent risk in holding data outside an organisation
	not all cloud app activities have equal risk
	activities that are benign for one role may be malicious in another
	it's risky activities rather than apps which should be blocked
	ACCTS_guide_2015 evidence from breaches e.g.. Target that long term companies rebound from breaches if they have the financial resilience and have handled communications well (i.e.. the key is not to produce a 'bad' customer experience)
	ACCTS_guide_2013 case study of small orgs not thinking they have data of interest to hackers -- different assessment of risk once considering willingness to just give away all their data.
	ACCTS_guide_2013 suggested measure of risk - willingness to share
	ACCTS_guide_2013 all data has value - to other people
	ACCTS_guide_2013 risk defined by the value of an information asset to anyone
	SP\12SEC reputational risk to web hosting/network service/ISP from which malicious activity is emanating - customers in breach of service
	ICO_2 maximum possible penalty £500000, applied where there is a serious contravention to DPA, that significant damages/distress may have been caused to the data subjects and either the breach was deliberate or foreseeable (risk known, likely damages known, reasonable steps not taken)
	penalties must be justified and proportionate
	impact on the data controller considered - their ability to pay "without causing undue financial hardship"
	Penalties can be enforced by county court if required
	ICO_1 undertakings followed two security breaches
	ICO questions commitment of council to protect data
	The council got a fixed period in which to make improvements
	No financial penalty was applied
	ICO_2 website breached by cyber attack (targeted by activist)
	ICO_3 ICO takes into consideration the number of sites/scope of vulnerability when making decisions - more impactful as 75 sites with the same problem, meaning higher risk of breach
	ICO_4 lost sensitive personal data (rather than credentials) results in an ongoing unmitigated risk
	ICO_5 legacy infrastructure was not decommissioned / data copied before new infrastructure installed to de-risk a project/business continuity however the risk to business continuity was overestimated and the risk of cyber breach underestimated
Supply Chain	*concern about the quality of cyber security in small organisations in the supply chain*
	push for basic security as criteria for contract
	risk shared/assumed by suppliers reducing incentive (banks)
	need speed/efficiency of interconnected systems to be competitive
	cyber stats offered inaccurate or imprecise
	cyber standards as badges of quality
	monitoring/notification/remediation through supply chain
	SP\9 no government contracts without accreditation in cyber security
	SP\10 cyber a perceived risk in small orgs
	SP\15 risk shared with suppliers - banks - reducing incentive
	ACCTS_guide_2013 highlights process/system speed and interconnected customers as the incentive to secure
	ACCTS_guide_2013 frequent use of BIS statistics and ICO fine thresholds

Supply Chain contd.	SP\9SEC a standards badge can be used to demonstrate that the company takes security seriously
	SP\12SEC law enforcement notification hopes to ensure regular monitoring and promote remediation
	SP\12SEC participation by notifying customers can reduce the cost to participant, customer and make the world a safer place
Data Protection	*reputation equivalent to customer trust*
	small organisations have incentive if knowingly under attack/being sanctioned
	overseas outsourcing introduces jurisdictional risk
	managing selection of data controllers as a privacy measure
	virtual organisations with low knowledge can demonstrate poor practices
	definition poor practice - hold data too long; publish data more widely than allowed etc.
	DPA/cyber synonymous in much advice
	government "official" accreditation an asset/badge
	virtual organisations use insecure home networks
	understanding lifetime of data uploaded and deleted from the cloud
	trend towards protecting critical assets
	ICO name and shame not a universal incentive - enforcement notice after failure to complete undertakings
	penalties take 15-27 months to be issued
	ICO decisions take account of impact on subjects
	employee mistakes contribute as much as malicious action to the success of breaches
	ICO focus on breach-stopping rather than attack-stopping measures (encryption)
	malicious activity a mitigating factor in ICO rulings
	negative impact - privacy vs financial details
	pervasive problems have higher magnitude
	supply chain protected in legal action - only data controller named
	expectation of security testing
	vulnerabilities on bespoke software not treated as avoidable zero days
	mistakes can nullify any appropriate security measures
	clarity of choice - limitations in data protection ability to protect consumers. When users state that their data can't be shared it can still be sold on as an asset of the company.
	the ability of virtual (committee-led) organisations to implement data protection
	SSITU.SP\8 small orgs knowingly under attack or facing sanctions have security incentive
	SP\10 reputation is reliant on customer trust
	SSITU\14 small organisation holding pseudonymised sample of 10% of the UK's medical data, plus identifiable military employee medical records. Network classified Official
	SSITU\14 data farm accredited for Official is a USP for private sector customers
	SSITU\14 suppliers with accredited systems and good data protection records gain referrals post-incident
	SSITU\16 privacy aware users manage the location of 3rd-party data to limit copies
	SSITU\16 cheap overseas outsourcing introduces risk due to lack of jurisdiction
	SSITU\19 charities/clubs can lack knowledge of data protection
	SSITU\19 committee-led organisations can lack continuity - data left in legacy systems either in more copies than needed or under the control of non-members
	SSITU\19 a lack of knowledge can result in inappropriate data use during the evolution/digitisation of legacy business processes (holding personal records too long, publishing members lists etc.
	SSITU\19 committee members in voluntary organisations use home devices for administrative tasks with no IT/security policies or controls implemented
	SSITU\19 committee led organisations lack knowledge of the lifespan of deleted files when using cloud services
	ACCTS_guide_2015 driving a trend towards the discovery and increased security of critical data
	ACCTS_guide_2013 advice on data protection integrated with cyber advice
	ICO_1 enforcement notice after 2 failures to acceptably complete undertakings. Questionable commitment to make changes and self evident likelihood of distress to data subjects if the council have a further breach

Data Protection contd.

undertakings followed two security breaches
European convention on human rights: the Council's data subjects have the right to respect for private and family life, home and correspondence
9 clear instructions have been issued, of which 4 have relevance to cyber security, 2 would create electronic logs and the remaining are procedural.

The council got a fixed period in which to make improvements
No financial penalty was applied
ICO_2 monetary penalty £200000, payable within 1 month, £160000 if paid before on or the last day of the month (forfeit right to appeal)
approx. 9900 individuals effected
personal data but no medical data breached
context of limited medical services offered by charity make it easy to assume medical reasons for communication
penalty took 2 years to be issued
ICO_3 monetary penalty £180000, payable within 1 month + 2 days, £144000 if paid before on or the last day of the month (forfeit right to appeal)
Hard drive used for backups misplaced
Should have been locked in a fireproof safe
had not been password protected or encrypted
information related to 2935 prisoners, including personal data and intelligence information
an identical breach had occurred previously in a different prison and remediation was supposed to have been completed
penalty took 15 months to be issued
ICO_4 monetary penalty £80000 payable within 1 month and 3 days reduced to £64000 if paid at least 1 day in advance, but with loss of right to appeal

unencrypted USB stick containing information about 286 potentially vulnerable children taken while unattended
reports are all protectively marked.
not found - ongoing risk
can't determine if there has been unauthorised access
took 27 months to be issued
ICO_5 undertaking
member of the public hacked a database
unencrypted
legacy server outside of the core infrastructure of the current website
>1M customer account details - no financial information
no evidence data was disclosed
attacker bypassed security measures undetected
penetration tests focussed on the new infrastructure
took 8 months to be issued
ICO_6 undertaking
4200 sets of personal data
in the creation of a new website a file containing personal data was unintentionally placed on the internet
this was not the first mistake made by the NHS trust in handling data that year - letter sent to wrong address
no monetary penalty was issued as the data controller has adequate "data processor" contracts in place - genuine mistake
took 16 months to be issued
ICO_7 undertaking
970 people - hospitality details
stolen laptop in an unlocked hotel room
password protected by unencrypted and not physically secured
passport data collected for all people irrespective of need, then retained in case of emergency
took 14 months to be issued
ICO_8 undertaking
hacking

Data Protection contd.

677335 data subjects registration details but no financial data
took 8 months to be issued
ICO_9 monetary penalty £160000
unencrypted DVDs lost during an office move
identifiable and distressing video of 1 sexual abuse victim, also identifying the perpetrators
lacked policy for storing this data in police stations
loss of the data was detrimental to the victim as the police had to request a second interview, but the outcome of the case was not effected
a complaint was made by the victim to the data controller as the outcome could have been impacted by their loss of evidence
the controller did not take appropriate action to protect against unauthorised processing and loss - procedures such as centralised storage
this type of information should have had the highest levels of security, the loss would have caused substantial distress and the data controller should have known better
took 21 months for penalty to be issued, BUT 22 months for it to be reported to the ICO
ICO_10 monetary penalty £175000
Online insurance company (specialist - travel insurance)
approximately 3M subjects, only 110096 sets of card details were live
data lost included credit card details and CVV
website was vulnerable due to lack of policy for applying security updates to CMS - this type of vulnerability had existed for 3 years
some of the legacy data was not encrypted
data which was encrypted was not protected as attackers gained access to keys
CVVs were kept to facilitate renewals, but policy was changed
project to delete and cease storing CVVs was not completed - human error
most transactions were transferred to a different system which did not require the storage of card details
fraudulent activity was carried out
multiple IP addresses accessed the compromised server
16 months to issue penalty
ICO_11 monetary penalty 180000
number of records stolen obfuscated
financial details part of stolen data
a server was stolen during a burglary - data accessible by a "motivated user"
policy not fit for purpose as physical security measures could not be implemented in a large number of stores too small to have a room to lock the servers in
another server was stolen from a 3rd party courier in transit
this server was only partially encrypted and could be accessed with forensic knowledge
servers not recovered
took 16 months to issue
ICO_12 monetary penalty 150000
online travel agent
the vulnerability which suppled an attack vector had existed since the code was written 6 years before the attack ZERO DAY ON BESPOKE SOFTWARE?
the website was penetration/vulnerability tested as it was not externally facing, but it was available on the internet
the attacker targeted financial details. CVVs were not available but the attacker targeted credit card numbers, names, addresses etc.
1163996 sets of details were compromised, 430599 current
no details had ever been deleted
the site was tested for functionality but not security OWN FAULT AS BOTH DEVELOPER/USER
a routine server check revealed an antivirus notification which highlighted the breach, 3 days after it started LACK OF MONITORING
took 19 months to issue
ICO_13 undertaking
independent estate agent

Data Protection contd.	an ftp server was poorly configured allowing anonymous access
	server had been indexed by google
	personal data relating to 41 clients could be accessed
	access had been available for 7 months
	data included some financial details
	company had no DPA training methods
	18 months to issue
	ICO_14 monetary penalty 7500
	in-house developed website
	hotel bookings
	during setup/install a WordPress server had been located in the same server as the web page
	the injection was used to extract wordblog password hashes - one password was hacked due to a marketing administrator using a default password
	APPROPRIATE SECURITY MEASURES NULLIFIED
	took 10 days to discover
	took 16 months to issue
	no security checks on site before launch
	vulnerability existed for 3 years
	developers lacked security training and lacked oversight
	3,814 client data
	card details encrypted but keys stored on the same server SIZE = NO NEED FOR >1 SERVER.... Understanding of security?
Reputation	*perceived insecurity damaging to product vendors*
	reputation is everything - income dependent on trust
	reliance on customer trust
	reputational damage of unnecessarily holding data
	penalties for data controller not root cause of a breach (suppliers)
	IT-driven models encourage continued interaction
	customers expect security in tangible products
	continuity and stability of service
	social media reputation is hard to manage - account ownership and 3rd party created content
	attempt to define reasonable care in services pre-emptively in case of breach to protect shareholders
	trust - the willingness to work with partners in the supply chain rather than accepting transferred risk
	SP\2 damage of perceived cyber threat in products
	SSITU.SP\8 need to achieve continuity and stability to preserve reputation
	SP\10 need sufficient security to maintain credibility when livelihood dependent on trust and confidentiality
	SSITU.SP\19 social media poses a risk due to inability to vet employee/volunteer posts before they go live
	MP1 low acceptance of faults makes safety risk more damaging than cyber risk - different expectations
	ICO_2 charity relies on trust/reputation to function effectively
	ICO_2 fact that data held unnecessarily could have damaged reputation further except report published long after breach
	ICO_2 delay from breach to issue of penalty of 2 years - additional press causing damage, vs full details not published until later
	ICO_2 the web companies who built and maintained the BPAS site are not named in the penalty alongside BPAS
	BBC_TalkTalk TalkTalk has limited the ability of customers to walk away in order to protect their shareholders / share prices
Threats	*threats evolving*
	government has visibility of credible threats to SMEs
	high risk customers are those subject to targeted attacks
	economic risk of widespread attacks
	questionable impact of commodity threats
	increased attack prevalence
	security measure effectiveness

Threats contd.

security arms race
threat to CNI from home IoT
moderately serious incidents where security outsourced to novices
complexity makes resilience hard
employees susceptible to social engineering
services used by small organisations lack security
employees try to DIY remediation rather than reporting incidents
expect free software templates - threat of including malware in a website as it is built
low resource lack resilience and limits ability to carry out good practice
customer poor practice is a risk to other customers
law enforcement can't mitigate against victim's lack of investment/interest in cyber security
reasons for attacks becoming more diverse
impact of breaches growing
international co-operation needed to tackle pervasive commodity threats
data feeds about threats available
magnitude of problem vs sophistication
organisation/attacker capability gap growing
alarmist headlines disincentivise
press overestimates the impact of a breach
vulnerabilities can be identified using readily available tools
staff may lack knowledge to act when a breach occurs
successful attacks the result of Swiss cheese security
website used as the 1st place to attack
SQL injection
CMS/web server vulnerabilities
poor practice: weak passwords/accounts; no patching; failure to keep knowledge up to date; failure to protect encryption keys
lack of understanding of the system as a whole - individual measures incomplete
multi-step attacks exploiting small vulnerabilities
SP\2 threats evolving
SSITU\5 other SMEs in shared network with poor practices
SSITU\5 profile of security company
SSITU.SP\8 targeted attacks aimed at high-risk customers
SP\9 government sees credible cyber threat to SMEs
SP\9 level of threat questionable when attacks are not targeted
SP\9 economic risk of widespread small-scale threats
SP\10 questionable threat to small organisations
SP\10 increase in the prevalence of attacks
SP\10 question of the efficacy of employing security measures in an evolving arms race
RH\11 threat to CNI via connected home IoT
SP\14 moderately serious incidents seen where IT outsourced to security novices
SP\14 employees failing to report incidents and attempting DIY remediation
SP\14 complexity of backups and minor data loss where malware attacks all drives - local, networked and shared
SP\14 employee susceptibility to social engineering
SP\15 victims can only be reliably identified for notification via financial links - e.g.. the ISP
SP\15 inexpert website construction might include compromised elements from the outset
SP\15 lack of security in services used by small organisations
SSITU.SP\19 luck and vigilance - single person companies can't monitor 24/7/365 and may be on holiday when a patch is needed
SSITU.SP\19 incident from one customer resulted in blacklisting and so continuity issues - consequence for all customers

Threats contd.

SP\20 single person company lacking interest in cyber lost company despite contacting law enforcement due to lack of self-protection
ACCTS_guide_2015 the impact of breaches is growing
ACCTS_guide_2015 the reasons for attacks is becoming more diverse
ACCTS_guide_2015 companies are experiencing record numbers of attacks
ACCTS_guide_2015 increase in the impact of breaches
ACCTS_guide_2015 encouraging developments in law enforcement where international co-operation can bring down botnets etc. to stop the spread of a specific kind of malware for a short period
ACCTS_guide_2015 economic growth means diversification of activities, which creates new threats
ACCTS_guide_2015 the gap between business and attacker capabilities is growing.
ACCTS_guide_2013 smaller organisations are increasingly being seen as a soft target
ACCTS_guide_2013 admitting that threats "may not be as devastating as the headlines suggest"
ACCTS_guide_2013 need to defend cyber against alarmist headlines
SP\9SEC commodity threat = "attacks using software and techniques freely available on the internet"
SP\12SEC data feeds in the public domain contain information about malicious activity
ICO_1 council reported two security breaches
ICO_2
- automated and readily available tool used to identify website vulnerabilities
- attempts made to gain unauthorised access to the website CMS
- website defaced
- staff aware of breach due to defacement
- staff were not aware of data being collected due to lack of understanding of their own systems
- staff did not have adequate measures for protecting administrator account details for the sensitivity of the data collected
- BPAS was not treating the data with the level of confidentiality they promised their customers
- vulnerability testing was not carried out
- website was not updated
- encryption was not implemented between the users and the web server

ICO_8
- internet-based SQL injection attack
- attacker gained access to the customer database
- breach possible due to vulnerability in the website code
- failure to apply up to date patches
- failure to arrange regular security (penetration) testing - no attempt to keep abreast of security developments

ICO_10
- website sustained an attack over a 14 day period
- attack exploited a vulnerability in the JBoss Application Server
- Attacker injected a malicious javascript webpage into the site
- backdoor was created to server
- ability to modify website and access backend database
- attackers has command shell access to give commands to the OS
- having access to the entire system allowed attackers to identify encryption keys
- attack was discovered by the card acquirer due to suspicious activity

ICO_12
- a single server contained an internal program (accessible by a website), the main website and customer data
- the staff website contained an error in the authentication scripts
- error allowed attacker to bypass authentication using SQL injection, logging into the admin interface
- by uploading malicious web shells to the site the attacker managed to gain administrative access to all the data held on the machine
- the attacker was able to access and edit files with the virtual network - the customer database and files used to process payment cards
- an exploit queried the customer database and used the insecurely stored encryption key to decrypt cardholder data

Threats contd.	attack took 3 days to detect data controller 'locked down' website to stop further data leaks ICO_14 vulnerability in the code which retrieved rate information which did not validate input the attacker used SQL injection content of the web page varied depending on the injection allowing extraction of the data character by character the injection was used to extract wordblog password hashes - one password was hacked due to a marketing administrator using a default password the attacker used the password to log into WordPress and alter templates to include malicious code, providing a gateway the gateway provided a convenient method to access all data on server blind SQL injection attempts on the credit card and internal mail account tables of the data controller's database card details encrypted but keys stored on the same server
Threat Intelligence	*intelligence/overviews help identify criminal networks* *providers aware of incidents happening* *threat intel produced by large organisations* *small orgs lack capability/capacity* *stories/case studies of attacks needed* *threat intel on small organisations currently comes from information sharing* *information sharing equivalent to peer support - poor branding* *BIS breaches have selection bias* *need economies of scale in producing threat intel* *security organisations use data collected from small IT users for own intel, but don't share intel with users* *ICO provides some data but decisions are subjective* SP\7 aware of cyber incidents that have occurred in the incubator SP\9 initiatives include providing example threats SP\10 abstraction in decision making until attacks come too close to home SP\10 justification for employing security SP\10 "good war stories" needed to help decision making SP\12 law enforcement can give credible information to infected users SP\12 threat overview helps ID cyber criminals - bad badness vs enablement via lack of awareness SP\12 making it normal to release attack information would allow users to adapt to threats RH.SP\13 UK overview of who faces threats RH.SP\13 global situational awareness RH.SP\13 threat intelligence about small organisations predominantly comes from the information sharing partnership RH.SP\13 information sharing provides peer-support RH.SP\13 small organisations lack capability to produce threat intelligence - some samples can be passed on for analysis SSITU\14 small-scale service provision introduced for economies of scale give provider extra threat intelligence through oversight SP\15 data on victims skewed by volume of spam relays BIS_breaches_2013 SMEs are included in the BIS information security breaches survey, although other small organisations are not defined separately ICO_actions_2015 Accounts of specific attacks carried out against small organisations can also be seen in the monetary penalty reports published by the UK information commissioner's office. This means that there is some limited evidence of attacks being carried out against small organisations and home users. This evidence may serve as motivation to improve security, however, records of the financial impact of an attack are subjective and would vary should the same attack happen to a victim in a different user group, making interpretation of the information difficult.
Security Capability	*threats proportionate to capacity to secure* *products' low detection rates reduce incentive* *high risk customers lose support* *capability might be measured on level of understanding of adversary* *expect/assume products are relatively secure* *outrunning each other as risk mitigation?* *ability of virtual organisations to secure themselves?*

		Security Capability contd.	*consumer clarity of choice - PPI as company assets to be sold on with the organisation*
			SP\2 consumer expectation of secure design
			SSITU\3 lack incentive as products ineffective at detecting infections
			SP\12 core message "understand your adversary"
			SSITU.SP\19 service withdrawn from high risk customers - those displaying poor practices which have had consequences for the supplier
			Expectation that organisations are trying to outrun each other rather than the bear
			small organisations behind in the arms race?
			Government and certain large companies are particularly worried about securing the supply chain -- the same argument from the opposite perspective -- risks held by government are controlled by their suppliers.
Threat Incentives			*Discuss problems with information in all sectors -- business incentives to share data? lawful publication of attack data collected for intelligence purposes. Mention of the number of SMEs in survey having trouble gauging level of threat without credible information sources.*
			Definitions of commodity threats/targeted?
			There is also (anecdotal) evidence of small charities or businesses who are linked to contentious political views being targeted by highly resourced attackers: activist groups or nation states.
			Scope for automation?
			Fashion in attacks?
	Attacker Incentive	User vulnerability	*reliance on internet services makes ssitu vulnerable*
			low knowledge increases return/persistence
			high availability of information about small-scale IT users
			SP\9SEC reliance on internet increases opportunities
		System vulnerability	*long term persistence*
			high value customer risks available through suppliers
			small orgs behind in security arms race
			visibility of assets increases incentive
			SP\10 some members may be unaware of breaches - longer term persistence
		Inexpensive exploitation	*exploitation of resource for attacks*
			ability to increase return on investment
			ability to reuse exploits
			ease of exploit of small orgs
			ease of exploit of small-scale IT user cyber footprints for social engineering
			scope to automate
			fashion in attacks
			low investment attacks
			SSITU\14 questions how change in profile/visibility of assets will impact attacks
			SP\15 social engineering by email offers big returns - reuse over wide audience
			SP\15 small organisations could be easier to exploit as botnets/relays
			SP\15 intersection of cyber footprints in small organisations - ease of social engineering (home/merged profile) plus bigger return (business)
			SP\15 complexity in a person's cyber footprint making it easier to obtain detailed information for social engineering to seem credible
		Motivation	*revenge for non-cyber activity*
			anti-competitive actions
			fraud - financial; ID theft or CC fraud
			espionage
			IP theft
			connectivity provides path to information
			risk high value credentials to perpetrate fraud against large organisations
			infrastructure is a valuable resource
			activism against contentious sectors
			highly motivated attackers in some groups

	Motivation contd.	*punishing entry level crime to reduce incentive*
		SP\12 prevention of escalation by punishing minor crime and increasing knowledge of legality and ethics
		MP1 Attackers may also be motivated by revenge for actions taken in the physical world, for example, the SME paper highlighted an example in one SME: ``We have come under attack from Far Eastern and other competitors due to legal action taken by us in connection with Intellectual Property''
		SP\9SEC threats = fraud, industrial espionage and theft of IP --- no mention of IT resource gain
		SP\12SEC law enforcement focus on infrastructure being repurposed by attackers
		ICO_2 targeted attack from anti-abortion activist
		ICO_2 the attacker found data about customers which he did not expect to find, increasing the value of the breach to the attacker
		ICO_(not 2) most incentivised by stealing usable credit card details, or stealing hardware for sale
TTPs		*only opportunistic attempts observed in home networks*
		spam
		spam friend requests
		commodity threats
		background noise
		unauthorised users
		ease of detection
		attack sophistication
		brand impersonation
		website impersonation
		human in the loop
		high number if iterative steps
		compromised 'free' software components
		SSITU\1 only opportunistic or commodity threat seen in home network
		SSITU\3 spam
		SSITU\4 spam friend requests on social media
		SSITU\4 unauthorised access attempts on WiFi from neighbours
		SP\10 routine threats
		SSITU\14 currently only commodity threats
		SSITU\14 majority of attacks are background noise, easily detected and blocked
		SSITU\14 past successful attacks due to unpatched vulnerabilities, driveby download or increasingly social engineering
		SSITU\14 social engineering by email - website with brand impersonation, user interaction over multiple steps, downloaded file resulting in ransomware
		SSITU\14 malware that can avoid signature detection until second payload
		SSITU\14 contextually relevant social engineering via email, including attachments
		SP\15 banking organs that bypass authentication by impersonating the bank website. Human in the loop carries out manual steps to gain access to the real bank's website
		SP\15 compromised or vulnerable components for DIY websites
		SSITU.SP\19 use of email server as a spam relay
		SP\20 potential revictimisation of those not self-protecting - highlighted as vulnerable users
	Opportunistic attacks	*resource influences likelihood of success*
		vulnerability
		the potential for re-victimisation
		no mention or awareness of targeting in small orgs
		SSITU\4 no awareness of targeting
		SP\7 no targeting mentioned by startups
	Targeting	*used for revenge - cyber seen as a soft spot for SMEs*
		ssitu as an attack vector
		transfer of responsibility to SMEs without risk

		Targeting contd.	*def. targeting: accuracy of means of contact; level of invested resource*
			SP\8 high net work individual - stolen hardware
			SP\15 defined by the accuracy of means of contact - mailing lists vs autogenerated addresses. Date of compromise of mailing lists defined by accuracy
			SP\15 invested vs opportunistic attackers - corporate attackers tend to be invested
			MP2 supply chain risk seen as motivator but SMEs not feeling pressure to engage
Interaction/Interconnection	Managing Interactions	Contracts	*poor motivation of web developers to provide ongoing contracts*
			contracts need to represent expected behaviour
			contracts don't often mention security
			SSITU\4 terms and conditions offer no consumer protection
			SSITU\4 contracts don't impose security and suppliers aren't generally required to demonstrate security
			SSITU.SP\8 systemic problem with web developers only taking easy 1-off contracts
			RH\11 subcontractors have expected secure behaviour outlined in contract
			ACCTS_guide_2015 acquisitions of poorly secured companies and their integration can increase the exposure of an organisation
		Consumer Expectations	*expectation of flexibility in device use*
			expectation of supplier holding some responsibility for security
			expectation of transferred/shared liability for incidents
			expectation of intuitive devices/systems
			expectation of free security as a service
			expectation of adequate security from suppliers
			SP\5 incidents in landlord-supplied networks are the suppliers fault
			RH\11 work devices should allow more than work functions to improve flexibility/choice
			SP\12 trust in supplier responsibility/accountability in contracts
			MP1 user expectation: ready out of the box, clear instructions, always safe, evolution without price increases
		Consumer Expectations ctd.	Consumer Rights Legislation - goods and services 'fit for purpose' or 'reasonable care and skill'
			MP1 summary of legal obligations: intrinsic safety, ongoing protection, instructions a part of product
		Supply Chain Expectations	*acquisition of poorly secured orgs might introduce vulnerabilities*
			MP2 Small organisations will out of necessity accept proportionally higher risks than large organisations
		Standards	*accreditation of services should be those that matter to consumers - strong requirement from small orgs would motivate supplier*
			incentives to develop standards like interoperability and pooled resources
			development of standards extremely slow
			security not addresses in consumer safety standards
			standards change significantly over time
			ISO standards costs too much for small orgs to implement
			ISO standard allows for risk-based implementations
			cyber essentials prescriptive
			CE has some scope loopholes and unattainable in some environments
			CE is light touch beginning of the security process
			CE still too complex for some orgs
			CE easier for small orgs with process flexibility
			CE focused on reducing vulnerability to commodity threats
			safety standards in high risk environments include cyber security
			consumer safety behind the curve
			SP\2 incentives - interoperability, pooled resources but slow process
			SSITU.SP\8 change significantly over time
			SP\18 a need to address cyber security risk in safety standards

Standards contd.	SP\18 standards take time to develop, but complexity DIY development, novel functions and the incentive of marketing means that the marketplace moves more quickly
	SP\6 time consuming and expensive but flexible (risk based)
	SP\10 unsuitable for smaller orgs
	MP1 ISO 27002 has been adapted and adopted into other standards
	SP\6 perceived as short-cut accreditation by larger orgs
	SP\6 for SMEs
	SP\6 difficulties to implement: legacy systems, complex infrastructure - satellite offices on 3G etc.
	SP\6 simple, inflexible prescriptive
	SP\6 variable time to implement - 2 days to months
	SP\6 loopholes introduced due to lack of ownership in the cloud
	SP\6 easier for SMEs to implement - purchasing/system flexibility
	SP\6 incentive to implement - government mandate for contracts
	SSITU.SP\8 useful reminder to customers and will improve security
	SP\9 focus is goal rather than product orientated
	SP\9 aim to plug vulnerabilities to avoid commodity threats
	SP\10 not seen much uptake/interest in a sector thought to have good practices
	SP\9SEC 5 key controls
	SP\9SEC designed as 'light touch' and low cost
	SP\9SEC even with a good track record introducing a formal process can improve security - can identify weaknesses in the process
	SP\9SEC the start of a journey
	BlueGuide_2014 Liability shared by manufacturer, producers providing components of a product, distributors and sellers
	MOD_2014 MoD standard for safety management in defence systems now includes a section on cyber security and data integrity
	BSI61508 functional safety of programmable electronic safety-related systems has a security section, requiring hazard analyses to include the possibility of ``malevolent or unauthorised actions''
	MP1 difficulty establishing security/safety requirements in cross referenced standards
	BSI60950 IT equipment, an example of a consumer product with both safety regulation and inherent cyber security issues, also has its own safety standard
	MP1 CNI provides far greater motivation than IoT for security/safety regulation - repeating problem of magnitude vs volume of incidents
Compliance	*consumer rights and product liability the main forms of consumer protection in the UK*
	fitness for purpose, provision of services with reasonable care and skill and intrinsically safe
	ICO regularly imposes undertakings to implement supply chain compliance, security testing and governance
	price/value of compliance outprices security suppliers for small orgs
	complexity and degrees of separation make compliance harder to enforce
	accreditation specialised enough to require consultancy
	unenforceable rules as not viable to sack non-compliant contractors
	safety reaccreditation depends on perceived evolution
	over-regulation (eg mandating standards) has its own problems - checklist mentality
	Argument for keeping data within sovereign state / EU to enforce data protection.
	cyber essentials plus requires pen test - micro orgs on SOHO routers will have shared IP@ designated by ISP - difficult to legally define scope of test
	SP\6 prescriptive standards can lead to indiscriminate security
	SSITU.SP\8 many orgs fail to be re-accredited and have to employ an expert to advise on device/config updates
	SP\8 accrediting security experts is counterproductive, pushing them out of the price range of small orgs
	RH\11 compliance is harder to enforce down the supply chain
	RH\11 the quality of security reduces down the supply chain
	RH\11 it's not financially viable to sack non-compliant contractors for poor security practices
	RH\11 subcontractors have basic accreditation before being allowed access

	Compliance contd.	RH\11 limited resource of audits and enforcement down the supply chain
		SP\18 safety reaccreditation depends on the level of product evolution - displaying a justifiable requirement
		SP\18 cyber security tests as part of safety accreditation is dependent on the availability of suitable tests
		MP2 ICO different because aim to protect consumer from service providers of all sizes and provide incentive by defining risk
		Netskope_guide_2015 - use of cloud SaaS model
		suppliers should be certified to the standards that 'matter' to the user organisation
		cloud security certifications: SOC-1/SOC-2/SOC-3, SAS-70/SSAE-16, ISO27001, HIPPA, PCI-DSS, Safe Harbour Certified, TRUSTe
		ISO_5 undertaking imposed after breach: regular website and server penetration testing; new data protection policy including study of data retention/disposal; formal data protection training and regular refreshers; appropriate implementation of other security measures to protect data and ensure that it is only kept as long as necessary.
		ISO_6 undertaking imposed by ISO after breach: due diligence when selecting data processors; governance and oversight of projects which includes a data protection risk assessment in the inception of a project; the data controller needs a breach management plan (containment/recovery/notification), which should then be maintained; appropriate implementation of other security measures to protect data.
		ISO_7 undertaking imposed by ISO after breach: impose adequate contracts on data processors; ensure personal data is collected only for specific and valid purposes; appropriate implementation of other security measures to protect data.
		ISO_8 undertaking imposed by ISO after breach: implement appropriate (to the data risk) periodic security testing; implement password storage appropriate to industry standard; develop/implement an appropriate software and security updates policy; monitor compliance with data protection and IT security compliance; other appropriate security measures to protect data
		ICO_13 undertaking from ICO after breach: introduction of security awareness training; contractors should get clear instructions about required security; other appropriate security measures
Cross-organisational Communication		*info sharing the main source of intel about attacks to SMEs*
		info sharing gives threat snapshot to SMEs
		info sharing requires membership - identifiable
		members tend to share identity with intel
		lack of relevance of info in large orgs
		info sharing provides conduit to authority and peer support
		large orgs don't gain much from info sharing, small orgs think hey lack info to share and govt needs data to understand scope of problems
		information sharing about community and reporting about informing authority
		apathy about reporting due to expectation of action
		few actions taken by local police forces based on action fraud reports
		notification about telling small orgs of breaches
		notification labour intensive due to time required to identify victim
		notification used to encourage collaboration
		conduit to authority vs conduit to stats engine
	Information Sharing	SP\10 membership organisation used as platform for dialogue
		SP\12 partnership between CERT UK and law enforcement
		RH.SP\13 benefit from shared information higher for small orgs who do not have the established business processes to gather all the information themselves
		RH.SP\13 large organisations typically aware of threats - lack of relevance of information shared
		RH.SP\13 initiative provides threat snapshot. More relevant to members than government who have a broader overview.
		RH.SP\13 in the case of small organisations information sharing is the main source of intelligence
		RH.SP\13 information is usually shared in an identifiable format to provide context for an attack despite competitors also being members
		RH.SP\13 means of increasing cyber resilience and maintaining partnerships (remit)
		SSITU\14 conduit to authority, peer support and encouragement to report incidents
		SSITU\14 report vs support imbalance - those able to contribute gain less than others
	Reporting	SP\20 apathy in the community - lack of trust and likelihood that law enforcement act
		SP\20 local simplification of the process to encourage reporting

	Reporting contd.	SP\20 details of means to report anonymously
		SP\20 data analysed from action fraud reports but no actions taken
	Notification	SP\12 law enforcement notification of victims and advice
		SP\12SEC aim to disrupt criminality and improve infrastructure security, reduction in compromised and vulnerable systems
		SP\12SEC process describes a means for measuring success
		SP\12SEC informing network admins as overseers - position of influence
		SP\12SEC difficulty in identifying companies using whois data - notification resource intensive
		SP\12SEC inform, advise and encourage collaboration
Complexity	Complexity	*increased reliance on supply chain*
		system complexity increases reliance on supplier
		SSITU.SP\8 networks includes remote access for support from foreign offices
		SP\10 increasing levels of interconnection in the supply chain
		RH\11 IoT represents the potential for pervasive endpoints connected into a CNI
		RH\11 home networks are increasingly sophisticated
		RH\11 interdependencies are difficult to map, let alone monitor or understand the social
		SP\12 challenging to work out how to get law enforcement close enough to victims to inform them
		SSITU\16 virtual organisations can be vulnerable due to lack of ability to implement physical security
		MP1 No reduction in complexity with consumer CPS - just as complex as traditional problem but smaller budgets
Multi-use Systems		*multi-use home networks in all org sizes - differentiation at device level*
		increasingly sophisticated technology use
		small but distributed infrastructure
		complex interactions with supply chain
		difficulty in mapping interdependencies
		difficulty in implementing physical security when a virtual org
		introduction of safety hazards
		decrease in scope of system control
		modular design and division of labour
Multi-use Systems contd.		*complexity in security design*
		need to secure system of systems
		use of devices for multiple roles
		use of networks by actors with different purposes and requirements
		virtual organisations have no dedicated infrastructure
		use to process correlation may be at device or application level, or not differentiated at all
		network cohabitation
		BYOD or UYWD
	Network	SSITU\1 work (medium-sized company), home, family, teenagers
		SSITU\3 family, children, work (employee large org with dedicated devices)
		SSITU\4 home, work (single person company), partner
		SSITU.SP\5 SMEs cohabiting (run by micro org)
		SSITU\5 work (micro security company), home family, children
		SP\7 startups cohabiting (run by large org) part of large org network
		SSITU\16 home, work (employee large virtual organisation with dedicated devices), partner
		SSITU\19 club committee members (virtual organisation without dedicated devices), home, work
	Devices	RH\11 policy allows personal use of work devices to reduce security avoidance
		RH\11 user expectation of BYOD policy, freedom of use and full functionality
		SSITU\17 mobile device used for work on the move
		SSITU\17 laptop used for leisure, work and higher risk functions - banking, online shopping etc.
		SSITU\19 club committee members (virtual organisation without dedicated devices), home, work

	Credential re-use	SSITU\16 only weak authentication, introduces a privacy issue, vulnerable to MITM attacks and suspicion of the motivation of social media suppliers (aggregation)
	BYOD Policies	RH\11 user familiarity with device and applications
		RH\11 avoids needing duplicate devices when travelling
		RH\11 improves work/home transition
		RH\11 becoming easier to control work content by decoupling software from the platform
		RH\11 interoperability issue - not possible to have a single enterprise system across all platforms
		RH\11 controlling access easier now with RSA tokens
Supply Chain	Supply Chain	*increase of small orgs in supply chain due to division of labour*
		increase of use of IT driven service based business models
		threat of pervasive SME insecurity
		decentralised decision making about a system of systems
		lack of tech knowledge leads to gaps in services requested
		vulnerabilities can come from any part of lifecycle - contracts, transfer between suppliers, development, implementation etc.
		closer logical connections increase perceived need for security by SMEs
		distribution of assets (data etc.) across supply chain
		simplification of (lightweight) processes reflected in SSITU IT decisions
		small orgs fail to manage supply chain expectations
		small orgs have to operate at higher risk
		SP\9 threat of pervasive SME insecurity
		RH\11 short term contractors bring their own devices
		RH\11 security implemented by compliance
		MP1 IT-driven business models make it easier for SMEs to enter new marketplaces, increasing resource contraints
		TalkTalk breach Case Study…
		contract outlines consumer rights and DPA and jurisdiction - no advice on enforcement
		consumer contract puts emphasis on ways supplier can protect themselves from unreasonable types of risk and enforcement methods
		contract refuses to claim liability for many security issues
		response to breach included in attempt to pre-emptively define "reasonable care" as no financial loss in case of breach
		protection of shareholders by using size/power to define acceptable reaction of customers - fighting to end contract penalty free could result in unpaid bills being passed on for debt collection
		MP2 most security risks related to interactions with other organisations
		ACCTS_guide_2015 business data increasingly dispersed across supply chain
		ACCTS_guide_2015 new business activity is leading to greater reliance/risk in the supply chain
		ACCTS_guide_2015 integrating systems with suppliers can be seen to introduce new weaknesses
		ACCTS_guide_2015 government intervention in cyber risk is difficult due to speed and differing risk profiles in each sector - supply chains can coordinate security more effectively themselves
		ACCTS_guide_2015 large organisations put processes in place to improve security but transformations/acquisitions can disrupt this process leading to less progress than expected
		ICO_2 BPAS were not aware that call back data was being processed in their website, hosted by one IT company but developed by another (who they fired for poor performance)
		ICO_2 BPAS contracts wit suppliers did not comply with DPA
		ICO_3 suppliers carrying out requests without offering advice leading to poor configuration (encryption installed but not activated)
		ICO_6 undertaking issued due to mistake when an old supplier was transferring data to a new one. Suppliers not mentioned by name
		ICO_7 mistake made by data processor extremely: limited data protection provisions in data processor contract Data controller (Panasonic) had a comprehensive data protection policy, but it was not passed on to the subcontractor
		ICO_13 the breach occurred due to an installation error by a contractor - fault on the estate agent for not asking for security considerations or checking the system after installation
Infrastructure		*lack of clear responsibility in shared networks*

Infrastructure contd.		*configuration limitations in consumer devices*
		definition of high vs low infrastructure systems
		Biodiversity in IT systems and it's relevance to cyber security...?
		resource required to create 'most secure' configuration
		defining a perimeter for security?
		knowledgeable users choosing cabled connections from devices they want to secure
	Infrastructure	*low infrastructure organisations might have more consumer tech in a system with increased redundancy*
		NAT problems reduce options for network security for some consumer devices
		individuals/small orgs may have no network ownership = control stops with devices
		pre-internet small orgs may have legacy processes and lack awareness
		security professionals' assumption about small org networks don't match reality
		SSITU\1 IP address ranges allocated to each member of the family
		SSITU\1 cabled office for increased security
		SSITU\1 two offices for resilience
		SSITU\3 cabled office, WiFi for he rest of the house
		SP\7 network and some workstations offered as part of the office
		SP\15 attacked org: pre-internet org, lack awareness, minimal online presence, legacy processes, ISP routing, lack security or segregation
		SSITU\16 DMZ required for consumer devices that don't function with NAT
		SSITU\17 no network ownership - laptop and smartphone only
		SSITU\17 uses university network, open WiFi or 3G
		MP2 many service providers don't understand what an SME network looks like
		Large surface area of SSITUs makes permimeter security challenging
		SP\9SEC CE: perimeter, configuration, access control, malware protection, patches
	Vendor Choice	SSITU\1 preference for a single supplier (Mac) to improve interoperability and system security
		SSITU\3 vendor agnostic
		SSITU\16 Linux trusted, secure, event visibility
		SSITU\17 vendor agnostic
	Mobile Devices	*often only free apps used*
		SP\2 static (h/w) and dynamic (s/w) platforms
		SP\2 updates necessary due to evolving threats
		SSITU\4 reliance on inbuilt security
		RH\11 need to limit the app stores used to increase security
		RH\11 supply high-spec devices to encourage use
		RH\11 increase home working and make users' lives easier
		SSITU\17 only free apps used, with email and social media synced
		SSITU\17 relies on inbuilt security
	Routing	*SOHO routing the norm in small orgs*
		questionable security in SOHO routers (provided by ISP)
		addition of 2nd router where ISP not trusted
		ISP device required in network to provide connectivity
		SSITU\1 ISP SOHO company-wide
		SSITU\1 home double routing - questionable ISP router security
		SSITU\3 home router not ISP SOHO - questionable ISP router security
		SSITU\4 ISP SOHO
		SSITU\16 home double routing - questionable ISP router security
		physical security can't be relied on for virtual orgs
	Virtual Organisations	*virtual orgs - use 'public' infrastructure for work purpose allowing growth without large offices*
		clubs/charities may have no physical presence even for core services/systems

Virtual Organisations ctd.

larger virtual businesses will have small physical presence to house core systems/services
most single person companies have no dedicated offices so a high percentage of infrastructure not dedicated
low infrastructure organisations might use increased size to increase resilience
small orgs have proportionally higher interactions and service area than large orgs
protecting critical assets where a critical mass not reached?
SSITU\1 employees (medium-sized org) work from home, customer sites or 2 micro-offices
SSITU\16 large virtual organisation, work mainly from home. Physical security can't be relied upon
SSITU\19 client organisation - 12 employees, sales reps in different countries working from home
SSITU\19 clubs/charities often have no dedicated infrastructure - websites/data hosted in the cloud, admin done on personal devices

Outsourcing

MP2 most single person companies do not have dedicated offices and so no infrastructure
MP2 m-sized orgs either like a large org or low-infrastructure strategy
ssitu - broad use of cloud backups/data share/ collaboration
some automation of backups employed
lack of affordable secure cloud
lack of discussion about value exchange for use of free cloud services
cloud cheap and simple fro non-experts
experts question trust in cloud service providers
cloud improves continuity
some see no reason to risk data in cloud
lack of questions asked of providers where service available
cloud allows for small-scale service provision
highest value assets often credentials/reputation with other orgs - no control and provider won't perceive this as customer asset
potential vulnerabilities introduced by app ecosystems - usability reduces security
orgs might be using cloud services without realising
cloud providers should implement security measures better than or equal to your own
SSITU\1 family data share facilitates network segregation
SSITU\1 high cloud use in company makes company scalably low-infrastructure
SSITU\4 cloud storage, email, communication and profiles
SSITU\4 automated backups
SP\5 no security advice sought from network owner
SP\5 lack of affordable secure cloud
SP\8 in-house cloud services provide customers with better continuity than free suppliers
SP\8 cloud is cheap and simple for inexpert use
SP\10 cloud - questionable trust or security
SP\10 data held in-house - lack of trust
SSITU\14 no reason to risk data in the cloud - retain risk in-house
SSITU\14 small-scale service provision for economies of scale
SSITU\14 marketing aimed at unknowledgeable managers causes friction
SSITU\17 cloud email and webmail
SSITU.SP\19 small-scale service provision - hosting, backups, control, cost-benefit
MP2 The use of online services is another example if cyber risk from distributed systems
Netskope_guide_2015 - use of cloud SaaS model
even if you don't know it you probably are using cloud services
SaaS is the "most fragmented" type of cloud model
Cloud app ecosystems, where APIs allow the automated sharing of data between apps result in a need to control app use across an ecosystem - some ecosystem apps may not be as enterprise ready as the core ones

	Outsourcing contd.	CASBs work as a proxy for all traffic - business continuity issue of single point of failure? overlap with MDM? security issues with CASB circumventing encryption to identify data and enforce policies?
		ACCTS_guide_2013 cloud security providers should have measures at least equal to your own
		ACCTS_guide_2013 raises the issue of jurisdiction and legal rules
Security Measures	Technical measures	*ssitu can be vendor agnostic*
		those with security criteria in tech selection anti windows
		reliance on inbuilt security for mobile devices
		evolving threat to mobile
		need to patch/update/secure mobile devices
		security linked to app stores used
		SSITU\1 laptops encrypted with a separate admin account
		SSITU\1 network firewall
		SSITU\3 work machine has mandated measures
		SSITU\3 limited security product use
		SSITU\3 network firewall
		SSITU\4 antivirus
		SSITU\4 network firewall
		SSITU\4 client data encrypted
		SSITU\4 obscure file names
		SSITU\5 no automated patching across shared network
		SSITU\5 network firewall - single person company has duplicated security at home
		SP\7 startups employ questionable security
		SSITU.SP\8 attacked organisation had poor policies, no audit trail, no monitoring, data leaks on examination, lack of proactive attitude to security
		SSITU.SP\8 companies need tools to ID attacks as incentive to employ security measures
		SSITU.SP\8 client data encryption
		SSITU.SP\8 sophisticated network security
		SSITU.SP\8 no shared hosting
		SP\10 detection and response only established business process in large orgs
		SSITU\14 vigilance, monitoring for indicators of compromise
		SSITU\14 free open source tools from reputable sources
		SSITU\14 paid tool - end point logging, cheap and easy
		SSITU\14 monitoring GUI gives obvious indication when something is wrong
		SSITU\14 encrypted hard drives
		SSITU\16 double firewall
		SSITU\17 physical security - locking screen when walking away from device in public
		SSITU\17 auto-update
		SSITU\17 unaware of any 3rd party products
		SP\18 lack of applicable security products for the home that ensure safety, or availability of test methods to test credibility of new products
		SSITU.SP\19 can patch all 50+ websites within 2 hours of release
		SSITU.SP\19 proactive monitoring - less than 1 incident to escalate to host/year
		SP\20 law enforcement refers incidents to different people depending on cost of breach
		MP2 Some of the building blocks that make up these infrastructures are almost identical to those used in the home, typically at the network endpoint
		MP2 feasibility of asset mapping in a distributed part-owned system?
		Netskope_guide_2015 - use of cloud SaaS model
		CASB - cloud access security brokers - policy enforcement points placed between consumers and cloud vendors
		Measure *user* policy compliance
		single enforcement point - reduce complexity, prevent cloud data leakage, enforce continuous compliance

	Segregation	*some small orgs have separate work devices*
		ssitu often use personal devices for work
		owners of small orgs often have little work/life separation
		experts enforce logical separation of client infrastructure
		SSITU\1 visitor DMZ
		SSITU\1 separate work machine
		SSITU\3 personal use of work machine
		SSITU\3 no division of network
		SSITU\4 no work/life separation
		SSITU.SP\8 logical separation of clients, avoidance of shared hosting
		SSITU\16 separate work machine
	Secure Products	*product security has to be balanced against consumer expectations*
		strong reliance from small orgs on embedded security
		perception some brands are more secure
		quality of embedded security depends on product
		customisation creates a problem for tomorrow
		orgs are at the mercy of software providers vulnerabilities
		less penalisation for vulnerabilities in purchased software than vulnerabilities in own bespoke software - interactions (compliance)
		ability to respond to new vulnerabilities critical
		SP\3 security balanced against consumer expectation of freedom
		SSITU\3 Mac more secure
		SSITU\3 strong reliance on embedded security
		SSITU\14 embedded security depends on choice of technology
		SSITU.SP\19 security at the mercy of the quality of software selected and the number of vulnerabilities found
		SSITU.SP\19 customisation is creating a problem for tomorrow
		SSITU.SP\19 website functions limited - limited users can login, reducing risk
		MP1 details of system evolution
	Resilience	*small orgs might not be aware of resilience*
		backups often done to NAS drive/cloud
		resilience measures more likely to be implemented after attack
		government attempting to permeate cyber advice in supply chain to improve resilience
		SSITU\3 backups on a NAS drive or cloud
		SP\10 mainly employed by large orgs
		SP\10 small orgs not really aware of the risk - implemented after attack
		RH.SP\13 remit to improve national cyber resilience - permeate advice in the supply chain
Ownership/Control		*Big corp influencing sector evolution by service level they are willing to offer*
		IT providers turkeys voting for xmas to report incidents so hold responsibility in companies
		Current cyber model best adapted to large organisations
		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 customer data.
		What is the obligation to provide security where products and services are supplied?
		User created value - defining how a product is used - blurs ownership.
		paradox - "because we created it we control it" "is this a feature or a threat, a value or a bug?"
		polycentric governance models as a parallel elsewhere? example of problems in defining boundaries in risk ownership, liability and control
		question of data ownership in free services
	Ownership	*threat intelligence hard to produce - funds*
		evolution in definition of public data - streetview - and consent for use
		ability of DPA to protect consumers from aggregation via acquisition
		org identity linked to personal IDs

Ownership contd.		*cost of unmitigatable risk*
		lack of control of social media profile
		lack of control in cases of impersonation
		employers may want to control configs to improve security
		suppliers limit control with built in configs - usability for all reduces configurability
		in-house hosting can reduce config/policy complexity
		user controlled infrastructure may only be endpoints
		control depends on ownership or power relationship with owner
		CE compliance includes loopholes where control/ownership known to be an issue
		infrastructure ownership limits ability to even test quality of security
	Data	SP\15 the availability of information without user consent (e.g.. google streetview) makes some users easy targets of social engineering
		SSITU\16 distrust of service providers ability to respect data protection during acquisitions - lack of choice who data assets end up in the hands of
		MP2 The perceived complete ownership of devices by their manufacturers may limit the level of creativity with which they can be used
		SP\20 threat intelligence hard to produce - austerity budget cuts leaving regions siloed
		Netskope_guide_2015 - use of cloud SaaS model
		many apps specify that the *vendor* owns uploaded data potentially immediately violating data protection rules.
	Identity	SSITU.SP\8 lack of control or regulation of social media accounts - individual ownership
		SSITU\14 the most damaging incidents involve impersonation - incident out of the company's control and with reputational consequences
		SSITU\16 ability to publicly impersonate on Twitter
	Infrastructure	SSITU\1 limitations in device config where NAT is used
		RH\11 organisations need to control endpoint config to reduce overall vulnerability
		RH\11 organisational security measures on BYOD endpoints improves security but not the owner's conflict of interest
		SP\12 government can protect attack victims short-term, using sinkholes to prevent exfiltrated data to reach its target
		SSITU\14 quality of security improved by keeping things in-house to reduce complexity
		SSITU\17 ends at endpoint
		SSITU.SP\19 customers retain control of content on hosted websites
		SSITU.SP\19 managing sites in-house maintains security but limits freedom of service provider
		MP2 System control closely linked to the question of ownership in IT and so has relevance to decision making
		CyberEss_2014 the first version of cyber essentials puts externally supplied IT, including cloud, out of scope
		MP2 Corporate cyber security measures are often about the absolute control of an element of a system for which ownership is required
	Cyber Risk	*IT and security synonymous in small orgs*
		cyber risk owners for SMEs not just SMEs
		suppliers retain control of config - ability to desecure
		incentive to secure when victim /= org in control of vulnerability
		SP\5 can't carry out pen-tests etc. in shared networks
		SSITU.SP\8 decisions include assessing customer risk
		SP\9 UK Cyber Strategy highlights government as a cyber risk owner for small organisations - economic risk - producing an education requirement
		SP\10 IT and security synonymous in small orgs - level of trust and expertise?
		SP\12 law enforcement notification of victims with delay - encouraging businesses to use own business processes
		ACCTS_guide_2013 advice aimed at reducing risk of company, *plus* their customers and partners
	Responsibility	*notion of virtual landlords and tenant rights*
		suppliers attempt to limit liability
		question about user liability/responsibility - safety - ability to understand decisions
		distancing from responsibility to reduce cost
		scalability of available cyber solutions for small orgs
		virtual orgs dependent on host/supplier investment in security
		charities may have to reduce security requirement to gain services needed
		diffusion of responsibility from system complexity

	Responsibility contd.	*responsibility to secure as collective action*
		SP\15 liability of ISPs - incentive when host not victim? notion of virtual landlords
		SP\15 availability of information - overview of network by ISPs
		SSITU\16 configuration limits imposed by suppliers in devices
		SP\18 safety and liability - what should the public be responsible for, capability to understand
		SP\18 IoT in home - power - could be referred to ombudsman for consumer protection & third party definition of liability
		SP\18 liability should be defined at point of sale to avoid ambiguity
		SSITU.SP\19 forums using the club name are managed at a distance by members to avoid needing to moderate for abuse
		SSITU.SP\19 charities hosted for free as CSR will be difficult to rehome if business disbanded
		SP\12SEC promoting 'cyber health' and make UK safer/more secure *to conduct business*
		MP2 Even where standards are developed to promote a basic level of security in the supply chain the UK government recognise the problem of implementing security where infrastructure is not owned.
		MP2 funding sources scope security solutions for large organisations
		MP2 government sees cyber risk as an economic risk - SSITU security their remit too
		ACCTS_guide_2015 diffusion of responsibility - the outcome of breaches being the use of company machines to attack other organisations may disincentivise security as there is no direct financial loss to the primary victim
		ACCTS_guide_2015 question of the role of government/security suppliers in encouraging collective action
		ACCTS_guide_2013 responsibility to other companies as soon as you begin working with them
	Support	*support often sought post-incident*
		expectation of free support - no budget
		membership orgs can tailor/provide advice
		access to experts may depend on luck
		advice may be to spend on automated systems
		security professionals take their expertise home
		outsourced IT reduces the incentive to report incidents
		advice needs to be simple and consistent message
		security/recovery implemented to protect reputation
		hosting allows for continued support
		incoherent roles/responsibility between orgs leads to inconsistency and gaps
		need to consider cyber in all activities
		respectful advice
		inevitability of compromise
		starting point
		common/commodity threats
	Peers	*peer support - free mutual exchange of expertise in very small organisations*
		family - designated tech support
		false experts
		knowledge vacuum
		charities/clubs look for professional support
		SSITU\3 family expert - duty
		SSITU.SP\5 unqualified inter-SME support within the innovation centre community
		SP\7 remediation advice from other startups
		SSITU\16 family expert - support with social media - filtering for shocked/vulnerable users
		SSITU\16 attempt to train family about dangers of social engineering
		SSITU\17 family expert (fake expert) - security novice but the person most inclined to fix things
		SSITU.SP\19 club/charity volunteers often use tech they know - legacy systems, low usability, high knowledge required
		SSITU.SP\19 clubs - virtual organisations, committee run

Peers contd.	SSITU.SP\19 charities/clubs beyond professional support - lack knowledge, need extra time/advice - unrequested sanity checks periodically carried out due to risk of user error
Government	*government offer simple advice*
	government message repeated/clarified in context elsewhere
	goal to empower security decision makers
	ability to advise requires good visibility of threats
	government accreditation puts suppliers out of budget for ssitu
	SP\9 simple advice for consumers/SMEs online
	SP\10 as soon as a supplier is accredited via government initiative they go out of budget for small organisations
	SP\12 limited freedom to advise - liability and risk to vulnerable users
	SP\12 goal of DIY security in response to regular intelligence feeds
	RH.SP\13 advice available on abuse/threats to CNI and government departments
	RH.SP\13 advice given to large organisations expected to permeate the supply chain - lack of contact with SMEs
	SP\20 ability to advise requires understanding of attacker TTPs, better reporting and patterns of revictimization
Professionals	SSITU\1 expert dedicated role in company overlaps into home network
	SSITU\1 expertly configured family devices
	SSITU\4 outsourced patching and updates
	SP\7 no security advice sought by startups
	SP\7 network and workstations maintained by professionals
	SP\7 startups manage own servers inside of network
	SSITU.SP\8 advise customers to use easy plug and play solutions - expensive
	SSITU.SP\8 advise auto-patching to get 45% more patched within 5 days
	SSITU.SP\8 referrals after attacks of small orgs with poor practices - security seen as a nice to have
	SSITU.SP\8 requests for post-incident expert troubleshooting
	SSITU.SP\8 standards re-accreditation often needs expert advice
	SSITU.SP\8 micro-orgs often seek one off disaster recovery - as much advice for free as possible
	SP\10 membership organisation can tailor advice to specific roles
	SP\10 information security advice an incumbent role of membership organisation
	SP\10 advice needs to be a simple consistent message
	RH\11 outsourced IT reduces the reporting incentive
	SSITU\14 in-house IT team of 2 shared IT/sec role
	SSITU\14 professional support from someone personally invested in security
	SSITU.SP\19 availability of expert advice for charities/clubs/virtual organisations depends on membership, word of mouth and CSR from SMEs
	SSITU.SP\19 web developer - single person company run by senior IT professional
	SSITU.SP\19 security/backups provided as part of service to retain reputation
	SSITU.SP\19 hosting allows continued support of sites
	SSITU.SP\19 content management done by volunteers leads to gaps in backups - incoherent roles and responsibilities
	ACCTS_guide_2013 advice given to small organisations mirroring/building upon the BIS 10 steps to cyber security, aimed at larger organisations
	ACCTS_guide_2013 guide puts government advice into context with extra information at the relevant ability level for the user group
	ACCTS_guide_2015 have identified flags to advise members: to consider cyber in all activities, accept the inevitability of compromise, focus on critical information assets, know that most companies don't get the basics right.
	The flags highlight an improvement in cyber in the (mostly large) organisations involved
	ACCTS_guide_2013 not afraid to talk about technical aspects of the system (in layman's terms)
	ACCTS_guide_2013 manages to provide non- condescending advice - respecting members
	ACCTS_guide_2013 minimal security advised for BYOD
	ACCTS_guide_2013 aimed to reduce "common, low level threats"
	ACCTS_guide_2013 working out how your vital business processes use technology as a start point for security
	ACCTS_guide_2013 uses case studies from experts - advice well grounded in industry and to govt advice

	Professionals contd.	ACCTS_guide_2013 security is only as good as the weakest link
		Netskope_guide_2015 condescending - let us tell you what you couldn't possibly understand
	Initiatives	*immature capability to protect public from cyber threats*
		government lobby to increase awareness via word of mouth
		law enforcement testing strategies/defining role
		humans needed in the loop to differentiate victims/attackers
		initiatives test different strategies - outcome largely awareness
		past initiatives may have lacked stakeholder input
		SP\9 government department lobbying membership groups to pass on cyber security marketing messages
		SP\9 government department guides on asset identification continuity and cyber decision making
		SP\9 government department measuring the quality of security products via accreditation (out of price range of small organisations)
		SP\12 law enforcement 4Ps used in cyber security
		SP\12 law enforcement use of government abuse feeds to ID victims (other end of communications)
		SP\12 law enforcement - still need humans in the loop to differentiate bad badness from victims
		SP\15 law enforcement identification of compromises
		SSITU\16 Snowden-revealed surveillance unsurprising but lacks proportionality/justification
		SP\20 law enforcement visits about cyber attacks more likely for businesses - more productive
		SP\20 production of metrics to highlight patterns in revictimization (following methods used for tracking burglaries) after advice on self protection
		SP\20 cyber capability - protect against cyber crimes and online abuse - immature
		MP2 list of initiatives focusing on small organisations
		MP2 need diffusion of information to target audience via trusted sources
Partnership		*concern from large orgs a bigger driver than that of small orgs for change in cyber capabilities*
		partnership as CSR
		partnership between SMEs to increase service breadth
		government engagement an attempt to build relationships, increase resilience and improve response
		partnerships = complex ecosystem where law enforcement becomes a co-ordinator
		success more reliant on open communication than tools
		initiatives giving more traction with home decision makers than businesses
		SP\10 membership org works with government to develop initiatives and share information
		SP\12 law enforcement and industry to provide malware removal tools
		SP\12 law enforcement and ISP to notify customers of breach
		SP\12 regionality to focus on community relationships
		SP\12 aim to improve response to cyber threat / cyber resilience
		SP\12 partnerships help to improve knowledge of how to make security products appealing
		SP\12 free marketing opportunity - credibility by association
		SP\12 complex ecosystem - law enforcement may just be co-ordinator
		SP\12 success based on open communications and relationships more than tools
		RH.SP\13 complexity in the supply chain means only direct contact with SMEs actually providing CNI
		RH.SP\13 engagement key to preparing for major national incidents
		SSITU.SP\19 partnerships between SMEs to provide wholesale services - value add for marketing and web development companies
		SP\20 law enforcement trying to build relationship with the community to advise on cyber protect
	Engagement	*service providers have to see a business case to engage*
		poor engagement from SMEs
		SME bandwidth issue - complexity vs poor knowledge
		service providers have to see a business case emerge
		SP\9 government department engagement with end users via Twitter and correspondence
		SP\9 initiatives have had more success with consumers than small organisations
		SP\10 lack of engagement from SMEs who are busy running their businesses

		Engagement contd.	SP\10 requests for a "bluffers guide to security"
			SP\10 cyber discussions were led by larger orgs
			SP\10 SME round tables held but poorly attended
			SP\12 lack of engagement from small organisations
			SP\15 getting service providers to engage in sharing cyber responsibility is dependent on building a business case
			SP\20 small orgs failing to engage with cyber essentials due to its complexity and their lack of knowledge
		Roles	*users have a role in own security*
			law enforcement attempts initiatives to create mitigation at scale
			government still defining its role in cyber security
			law enforcement for most vulnerable infrastructure or people
			SP\2 users have a role in their own security
			RH.SP\13 remit to cover government departments and CNI so not public facing but also have to improve cyber maturity
			SP\15 immature environment - defining roles in relationships of reporting and detecting
		Self Protection	*information as an enabler*
			SP\12 aim to provide enough information to enable security
			SP\12 roles undefined - immature notification process
			SP\12 limited action by law enforcement to achieve mitigation at scale
			SP\12 law enforcement must only be used for most vulnerable infrastructure
			SP\15 law enforcement gives victims time to remediate to only use resource on chronic problems
Cyber Physical	Safety Risk	Safety Risk	*Constant evolution of cyberspace*
			Increasing interlink between physical and virtual world
			Scope to impact safety, economics, politics
			Speed of information flow
			Reliance on large orgs for research funds/problems and customers
			Microscopic focus of attack research
			Macroscopic study of IT models
			Lack of economy of scale
			Incomplete Small-Scale security model
			Rise in supply chain interconnectivity
			Increase in threats
			Accessibility of security measures?
			critical functions - healthcare etc. - best effort bandwidth versus precedent (electricity) to prioritise vulnerable users
			home network seen as hostile by risk-holding suppliers
			End users considered adversaries
			SP\18 IoT in the home faces challenge of integration, interoperability, complexity
			SP\18 introduction of critical functions to the home - questionable control over prioritisation
			SP\18 user expectation for product safety
			SP\18 testing often carried out without legal requirement to meet user expectation and protect reputation
			SP\18 IoT devices need to turn on safe without prior user knowledge
			SP\18 introduction of critical functions into home networks by IoT/telehealth without segregation/prioritisation/network availability guarantees
			SP\18 liability for/consequences of malfunction from remote access depends on degrees of separation
			MP1 risks to data integrity, of malfunction, and remote operation
			Information leakage -- real life information inadvertently leaked into the internet
	Internet of Things		*traversal of risk between virtual and physical realms - swatting (c-p)/revenge after legal action (p-c)*
			revenge without consequences
			liability hard with degree of separation
			expectation of safety
			introduction of home safety critical functions

Internet of Things contd.		*challenges of interoperability/complexity on integrating CPS*
		privacy erosion
		IoT devices not being segregated in home network or segregated at lower sec DMZ
		increased small stakeholders increases complexity and vulns for larger stakeholder
		evolution should augment performance
		innovations marketed as sexy
		need for safety accreditation model
		IoT currently mainly smart media devices
		rapid innovation of IoT devices
		questionable user control over remote updates
		business model ambiguity
		MP1 Requirements
		MP1 framework to be reconsidered at a later date?
		SSITU\1 active in unsegregated network
		RH\11 connection of IoT to CNI - resilience vs number of micro-stakeholders, complexity, lack of control and increased vulnerabilities
		RH\11 devices in the home make cyber crime easier - fraud against suppliers or DoS
		SSITU\16 risk of privacy erosion with the introduction of more intimate data collection
		SP\18 augment home performance, taking into account user comfort and safety, not just be a marketing exercise
		SP\18 rapid innovation and increase in number of connected home devices
		SP\18 questionable/immature security model, with a need for accreditation of security product accreditation
		SP\18 precedent - accreditation of smart meter security and expert testers by CESG
		SP\18 home automation currently marketed as sexy
		SP\18 IoT devices open to service evolution and increased capability
		SP\18 remote access increases cyber risk
		SP\18 questionable user control over updates/service changes implemented remotely
		SP\18 business model legal ambiguity/complexity - service or product depends on duration of consumer-manufacturer relationship and the level of manufacturer intervention during product lifecycle
		MP1 research into CCPS viewed consumer as malicious actor
	Consumer CPS	*MP1 consumer products containing embedded systems that take advantage of the increase in available wireless technologies to connect to the Internet*
		MP1 As computing becomes ubiquitous, the lines between IoT sectors are likely to blur as new services themselves provide new opportunities for services
		MP1 Consumer CPS likely to be developed in part by small competitively priced companies contracted by a manufacturer
		MP1 risk from consumers not considering the cyber risk of how they use cyber physical device
		MP1 environment has evolved
	Emerging IoT	SSITU\1 TVs, set top box, DVD, Xbox
	Unused Capability	SSITU\3 washing machine
		SSITU\4 DVD
		SSITU\16 TV - services not worth the data leak

D

APPENDIX D – THE COMPLETE SMALL-SCALE CYBER SECURITY REQUIREMENTS FRAMEWORK

This appendix presents the full versions of the requirements frameworks evaluated in Chapter 6. The SSITUs' requirement framework stands alone. The RHs' framework assumes the inclusion of all non project-driving requirements (1CO01, 1OW01 and 1OW02) from the SSITU framework and cross-references conflicting requirements from that framework.

The framework uses the requirements template components described in Chapter 3 with the addition of the cyber security process categories discussed in Chapter 6 as part of the requirement ID RID.

Requirement IDs: all requirements from the SSITU framework are prefixed 1 and the additional requirements in the supply chain RHs' framework are prefixed 2.

The categories (C) of cyber security principle are recorded as follows:

- Ownership — OW
- Context — CO
- Planning — PL
- Application — AP
- Adaptability — AD

The requirement sources are coded as follows:

- SSITU, SP, RH — one of the stakeholder groups
- ESYS — the small-scale cyber security ecosystem (a research outcome)
- LIT — either academic or standards literature
- G — UK Government

The 'P' column describes priority as discussed in Chapter 3:

- Critical (C)
- Important (I)
- Optional (O)
- Unchangeable constraint (X)

Table 20: *A cyber security requirements framework for SSITUs*

RID	C	Reqt Category	Requirement type	Description	Rationale	Src	Fit	P	Conflicts
11101	OW	Project Drivers	Project purpose	Government need to achieve a basic level of engagement with cyber security from all SSITUs - either implementing advised 'essentials' or complying with regulatory requirements.	Government hold responsibility for cyber security's risk to the national economy	ESYS		X	
10001	OW	Project Drivers	Stakeholders	Project owner is a SP (who may also be a SSITU)	SSITUs need improved cyber security but are not large enough to sponsor solution development uniquely for their organisation. There is scope for startup SSITUs to develop products/services for this sector.	ESYS	N/A	X	
10002	OW	Project Drivers	Stakeholders	SSITUs (or a subset) are the intended customer	SSITUs are the focus of this research	ESYS	N/A	X	
11106	OW	Design Constraints	Anticipated workplace environment	Incidents impacting on reputation are likely to be catastrophic for SSITUs	SSITUs lack the financial resilience of larger companies in case of reputation-damaging incident – limited cash flow	SSITU	N/A	X	
11132	OW	Non-Functional Requirements	Compliance	SMEs must comply with GDPR and exempt SSITU organisations often need to align themselves with GDPR	Majority of SSITUs hold some kind of personal information and even exempt organisations (except families and individuals) are concerned about being reported for data breaches	SSITU	Solution supports GDPR compliance	X	12251
11142	OW	Non-Functional Requirements	Capacity	SMEs need incentives to implement security	Currently cost-benefit analysis favours many SSITUs not engaging with cyber security	ESYS	SSITUs cyber security processes achieve 10003 or 10004 and statistics report increased cyber security engagement	C	
10003	OW	Non-Functional Requirements	Compliance	SSITUs need accountability as a catalyst for evolving formal processes	11117, 11118, 14401	RH/SP	SSITUs can name a person or organisation that would hold them accountable in the case of a breach	C	13307
11111	OW	Design Constraints	Cultural	SSITUs make decisions based on the expectation of supported services	10007, 12220	SP	Solution has support for novices as a component	X	11124, 11133
11133	OW	Design Constraints	Current system environment	The main SSITU service provider may also be a novice (network infrastructure)	SSITUs reported other SSITUs' expectations that incidents were their fault	SSITU	Solutions are implementable by novices	X	11111
11143	OW	Non-Functional Requirements	Compliance	GDPR only protects (living) individuals in a personal context, not all customers SPs consider 'consumers'	Legislation is intended to protect personal data, without taking into account the vulnerability of some business owners/operators	LIT		X	11131, 12212
11134	OW	Design Constraints	Current system environment	SSITUs lack ability to stop other system stakeholders altering configurations without permission	SPs control large amounts of a SSITU system and 11129	SSITU		X	
11144	OW	Design Constraints	Current system environment	SSITUs' most valuable assets to protect may be credentials for 3rd party services	Reputation is the biggest incentive to secure, resulting in SSITUs' concern over credentials for 3rd party services	SSITU		X	11129
11129	OW	Design Constraints	Current system environment	SSITUs have no influence over SLA/contract terms.	SSITUs are 'price-takers' and their suppliers tend to be far larger, with an expectation of being able to force terms on end users	SSITU		X	12251
11131	OW	Design Constraints	Current system environment	SMEs are treated as consumers	11129	ESYS		X	

RID	C	Reqt Category	Requirement type	Description	Rationale	Src	Fit	P	Conflicts
10004	OW	Non-Functional Requirements	Ease of use, understandability and politeness	SPs need to reduce the effort required for SSITUs to engage with cyber security	Currently cost-benefit analysis favours many SSITUs not engaging with cyber security	LIT	The solution is: a default setting; can be achieved and maintained by novices; or it becomes one of the security measures SSITUs consider a benchmark requirement for reasonable cyber security	C	11124, 11129
10008	OW	Non-Functional Requirements	Interfacing with adjacent systems	Influential members of the supply chain need to increase the cost of SSITUs not engaging with security	SSITUs are price-takers and so RH stakeholders/their security experts have suggested using their influence to force greater compliance	RH	SSITUs achieve a cyber security standard	C	10005, 10006, 11136
10007	CO	Design Constraints	Anticipated workplace environment	SSITUs are security aware but lack equivalent knowledge as decision makers	SSITU decision makers are not generally cyber security experts	SSITU		X	
11103	CO	Design Constraints	Anticipated workplace environment	There is a lack of cross-fertilisation of expertise between the cyber security and SME sectors, limiting SSITUs' access to experts	Cyber security experts, even cyber SMEs tend to adhere to perceived best practices and aim their services at larger customers. Inversely,11121	ESYS	Solutions are implementable by novices	X	
11104	CO	Design Constraints	Anticipated workplace environment	SSITUs have inconsistent access to cyber security knowledge	Internet penetration versus population with access to corporate cyber security training	SSITU	Solutions are implementable by novices	X	
11105	CO	Design Constraints	Anticipated workplace environment	There is less legal support available for SSITUs than for large organisations	Government/law enforcement can't protect at scale: the can't afford to support every business independently in case of incident, whereas they do investigate catastrophic (or high cost) incidents in large organisations.	RH/SP	N/A	X	
10005	CO	Non-Functional Requirements	Interfacing with adjacent systems	SSITUs need less perceived cyber security vulnerability to support self-efficacy	Self-efficacy is undermined by seemingly insurmountable problems	LIT	The solution is presented to the SSITU in a way that makes them certain that it will have a measured effect and they can easily implement it	C	10007, 11103, 11104, 11105
10006	CO	Non-Functional Requirements	Interfacing with adjacent systems	SSITUs need to feel that their engagement in cyber security will result in a catastrophic breach ceasing to be inevitable	11106, self-efficacy is undermined by a perceived lack of progress	LIT	There is a combination of solutions that allow SSITUs to comply with the most reputationally damaging of: GDPR; or customers' cyber security expectations.	C	13307 + 11106
11107	CO	Design Constraints	Anticipated workplace environment	SSITUs' day to day operation takes precedence over administrative/ housekeeping processes	SSITUs stating being busy "running their business" is a key factor in their lack of engagement in cyber security	SSITU	N/A	X	11132 + 11106
11135	CO	Design Constraints	Anticipated workplace environment	SSITUs are IT-dependent	Most SSITUs would struggle without their IT systems for more than 24 hours	SSITU	Solutions do not suggest that SSITUs cease to carry out any activity and adhere to 13319/ 13308 where possible	X	
11136	CO	Design Constraints	Anticipated workplace environment	SMEs have to accept risks where a security requirement stops business functioning (including by limiting their ability to accept contracts)	Small organisations are by definition high-risk and cannot survive if they do not accept high-risk opportunities	SSITU	Solutions do not suggest that SSITUs cease to carry out any activity and adhere to 13319/ 13308 where possible	X	11132

RID	C	Reqt Category	Requirement type	Description	Rationale	Src	Fit	P	Conflicts
11109	CO	Design Constraints	Anticipated workplace environment	SSITU organisational culture may be too informal to support rigid security processes	13316, 11114, 11116, 11117	SSITU	N/A	X	11132
11115	CO	Design Constraints	Current system environment	SSITUs use consumer devices or solutions in a business setting	The cost of entry for many business solutions is unaffordable for SSITUs	SSITU	Solutions are usable by individuals in a home environment	X	13315
11117	CO	Design Constraints	Current system environment	SSITUs' socio-technical processes will be undocumented	SSITUs have fewer formalised business processes than large organisations	SSITU	N/A	X	11132
11137	CO	Design Constraints	Anticipated workplace environment	There is more than one set of cyber security requirements in the SSITU group (they have been amalgamated to take the prevalence of multi-purpose systems into account)	There is complexity in the SSITU group - their diversity means their educational and technical needs are not identical	SSITU		X	
11138	CO	Design Constraints	Current system environment	SSITUs lack the critical mass to protect their highest-value assets	High-value' is proportional to the SSITU's total assets, not the cost of cyber security measures	SSITU		X	11132
11139	CO	Design Constraints	Current system environment	SSITU systems lack the artefacts many security measures are designed to protect	12234	SSITU		X	11132
11140	CO	Design Constraints	Customer budgetary constraints	SSITUs' assets are not of sufficient value to warrant security investment	Cost of entry too high for more than basic security measures	SSITU		X	11132
11141	CO	Design Constraints	Current system environment	SSITUs often have detailed, interconnected and non-reducible digital footprints	12237	SSITU		X	
12201	CO	Non-Functional Requirements	Access, integrity and privacy	Need to allow the option for SSITUs not to participate in supplier datasets/their aggregation, irrespective of individual/organisational status.	SSITUs protecting reputation through segregating/limiting digital footprint and 11131 + 11143	SSITU	Services offered to SSITUs must allow an opt-out of data collection or aggregation in line with data protection rules for individuals	I	11129, 11143
12216	CO	Non-Functional Requirements	Immunity	SSITUs need to reduce their vulnerability to social engineering	SSITUs' digital footprints can be extremely complete, making it far harder to identify social engineering	ESYS	Solution: does not introduce additional personal information into the public domain; may reduce the amount of aggregated personal information; or removes personal information from the public domain.	I	11129, 11141, 11143
11108	CO	Design Constraints	Anticipated workplace environment	SSITUs have inter-role conflicts of interest	SSITUs report using company/ home infrastructure for multiple purposes and are resistant to security policies that would preclude them completing all their required roles	SSITU	N/A	X	12251
11116	CO	Design Constraints	Current system environment	SSITUs may be entirely virtual, without dedicated devices or services	SSITUs described how some organisations were IT-dependent without supplying equipment or services	SSITU	N/A	X	12251
11124	CO	Design Constraints	Customer budgetary constraints	SSITUs' security budgets are not high enough for suppliers to want to offer well-supported high-effort solutions	SPs describe wanting to provide cost-effective (nothing difficult) solutions under rigid terms.	SP		X	11111
11125	CO	Design Constraints	Customer budgetary constraints	SPs offering hardware are incentivised to force customers to purchase devices more frequently, reducing the IT budget available for security	Evidence of smartphone manufacturers limiting the period of security updates so that updates cease before fixed contracts end	SP		X	

RID	C	Reqt Category	Requirement type	Description	Rationale	Src	Fit	P	Conflicts
11126	CO	Design Constraints	Customer budgetary constraints	Some SSITUs are inherently risky customers (high net worth individuals etc.), limiting the number of service providers willing to support them, irrespective of their higher budgets	SPs describe reducing services to risky customers to reduce their own risk	SP		X	
11127	CO	Design Constraints	Current system environment	SSITUs lack a coherent/focused IT strategy, often using multiple solutions for the same activity	Lack of influence over customer IT use – customers dictate format/means of data transmission. Lack rigid policy for employees	SSITU		X	12251
11128	CO	Design Constraints	Current system environment	Supply chain requirements limit SSITU choices	The supply chain dictate many SSITU system components, reducing the types of security they are able to employ	RH/SP		X	12251
11130	CO	Design Constraints	Current system environment	SSITUs are dependent on suppliers' quality of service	11129	SSITU		X	12251
12237	PL AP	Design Constraints	Anticipated workplace environment	It is not possible to segregate users' multiple roles for best-practice access control	For the majority of SSITUs there is no system, device or piece of software dedicated to one role	SSITU	Solutions anticipate devices and software being used for multiple roles	X	
12207	PL AP	Non-Functional Requirements	Cultural	SPs need to anticipate BYOD-style IT models	SSITUs' lack of economies of scale make multi-purpose devices/infrastructure the norm.	SSITU	Solutions anticipate devices and software being used for multiple roles	C	
12208	PL AP	Non-Functional Requirements	Cultural	SPs need to anticipate a multi-purpose IT system	11122	SSITU	Solutions anticipate devices and software being used for multiple roles	C	
12211	PL AP	Non-Functional Requirements	Cultural	Solution needs to protect the individual's right to freedom of Internet use to successfully secure very small organisations	12208	SSITU	The solution does not block the SSITU from being able to carry out activities in any role	C	
12209	PL AP	Non-Functional Requirements	Cultural	System users need to safeguard vulnerable users (not employees)	Multi-purpose systems are likely to contain vulnerable individuals (children etc.) despite also supporting businesses and adult use	SSITU	Solutions allow vulnerable users to be segregated from some activities	I	
11112	PL AP	Design Constraints	Current system environment	SSITUs may have no physical environment to secure.	The smallest SSITUs only rent work space when their job requires specialist equipment or services. SSITUs report a high level of organisation virtualisation.	SSITU	Solutions assume that the SSITU is working out of office	X	11132
11113	PL AP	Design Constraints	Current system environment	SSITUs are unlikely to have fixed networking infrastructure.	The size or distribution of some SSITUs make cloud services a more viable option	SSITU	Solutions assume that the SSITU is working out of office	X	11132
11114	PL AP	Design Constraints	Current system environment	SSITUs have high levels of home-working	A high proportion of SSITUs either run their business from home or attempt to reduce costs by allowing flexible working	SSITU	Solutions assume that the SSITU is working out of office	X	11132
12234	PL AP	Design Constraints	Anticipated workplace environment	SSITUs maintain a highly distributed IT system	Small-scale requirements combined with low knowledge, influence and budget, result in extensive use of 3rd party services	SSITU		X	11132
12235	PL AP	Design Constraints	Anticipated workplace environment	SSITUs have a proportionately large attack surface	12234	SSITU		X	
13323	PL AP	Design Constraints	Current system environment	SSITUs have limited control of system layers	11129	SSITU		X	11132

RID	C	Reqt Category	Requirement type	Description	Rationale	Src	Fit	P	Conflicts
13324	PL AP	Design Constraints	Current system environment	SSITUs lack the ability to employ multi-layered security models such as Defence-in-Depth	12234	ESYS		X	
13302	PL AP	Non-Functional Requirements	Access, integrity and privacy	SSITUs need to protect their data irrespective of its location	12234, 12240	SSITU	SPs maintain SSITUs' data in compliance with GDPR, even when the SSITU is a business rather than an individual	C	11143, 11129
13312	PL AP	Non-Functional Requirements	Expected physical environment	SSITUs need to achieve optimum security at the endpoints	Endpoints are likely to be the only element of the system controlled by the SSITU.	SSITU	Solutions do not require SSITUs to remove investment from endpoint security measures	C	11132
12225	PL AP	Non-Functional Requirements	New problems and migration	Solution designers need to recognise cyber threats as potential safety hazards in networked consumer CPS	The introduction of consumer CPS via the IoT could undermine existing product safety levels if cyber security is unaddressed	LIT	Cyber security is considered as an embedded service when IoT solutions are designed	I	
13304	PL AP	Non-Functional Requirements	Audit and documentation	SSITUs need more transparency from suppliers about the systems they provide	12218	ESYS	IT solutions are offered with transparency and suggestions of applicable security measures	I	
12247	PL AP	Design Constraints	Current system environment	Standards assume SSITUs have a physical environment	Standards are developed and maintained by larger organisations and so reflect their IT systems	LIT		X	11112, 11139
12248	PL AP	Design Constraints	Current system environment	Standards make tech-specific assumptions about the system they are being applied to	Standards are developed and maintained by larger organisations and so reflect their IT systems	LIT		X	11112-15, 11139, 12234 & 37, 13323
12251	PL AP	Non-Functional Requirements	Compliance	GDPR adopts the assumptions made by cyber security standards	GDPR makes reference to similar practices and suggests that standards compliance would be an acceptable means of demonstrating security	LIT		X	11112-15, 11139, 12234 & 37, 13323
12212	PL AP	Non-Functional Requirements	Cultural	Need to consider SSITUs as consumers with a requirement for GDPR compliance	11115, 11132	ESYS	The price of entry and prerequisite knowledge for the solution aligns with 11118 and 11104	C	11143
13305	PL AP	Non-Functional Requirements	Audit and documentation	SSITUs need to develop sufficient documentation to satisfy GDPR	11132	LIT	Solution allows SSITU to comply with GDPR	C	11109 & 17, 12251
13306	PL AP	Non-Functional Requirements	Capacity	SSITUs need to implement sufficient security measures to satisfy GDPR	11132	LIT	Solution allows SSITU to comply with GDPR	C	12251
13307	PL AP	Non-Functional Requirements	Capacity	SSITUs need to satisfy GDPR security requirements without having the prerequisite resources/ infrastructure to comply with the standards those requirements are based on	SSITUs' resource, infrastructure and system control are limited, but they still need to comply with GDPR.	SSITU	Solution allows SSITU to afford comply with GDPR without ceasing to operate	C	
13313	PL AP	Non-Functional Requirements	Immunity	SSITUs need to have enough (accessibly presented) system information to comply with GDPR monitoring requirements	11132	SSITU	Solutions automatically log sufficient information to comply with GDPR and either present this information in a user-friendly format or provide application interfaces to system monitoring software	C	10007, 11104, 11107

RID	C	Reqt Category	Requirement type	Description	Rationale	Src	Fit	P	Conflicts
13314	PL AP	Non-Functional Requirements	Interfacing with adjacent systems	SSITUs need to be able to identify and locate key assets within an organisation	Unavoidable best practice	LIT	SPs are transparent about where and how assets are maintained	C	11127
11102	PL AP	Non-Functional Requirements	Standards	SSITUs need to achieve the essence of cyber security standards without being able to comply with technical assumptions	12247, 12248 and to be competitive SSITUs need to find a sustainable way to engage with cyber security.	ESYS	SSITUs can demonstrate compliance with the high-level goals outlined in standards without necessarily implementing the technical measures advocated by the standard.	I	
12217	PL AP	Non-Functional Requirements	Interfacing with adjacent systems	SPs need to evaluate the level of virtualisation in how the SSITU operates to anticipate required security measures	Virtual organisations still have tangible assets to protect but have severely limited system control	SSITU	Solution is appropriate for a fully virtual organisation or clearly defines the operational context in which it is intended to be implemented	I	
12236		Design Constraints	Anticipated workplace environment	SSITUs are reliant on low-effort policy measures	Low resource measure	SSITU		X	
12218		Non-Functional Requirements	Interfacing with adjacent systems	SSITUs need to be able to identify a perimeter for security	If SSITUs have no comprehension of how they are using IT they cannot assess their risk	LIT	SSITUs have the capacity to enumerate their IT use and identify their assets	C	
12220		Non-Functional Requirements	Interfacing with adjacent systems	SSITUs expect shared responsibility with their suppliers	When an incident occurs SSITUs lose self-efficacy and suppliers may be their only access to expertise	SP	Solution has support for novices as a component	C	
12231		Non-Functional Requirements	Standards	SSITUs need to protect assets which are not under their control	The distribution of the system and focus on reputation makes it more likely that an SSITU's most valuable assets are not under their direct control	SSITU	12240 is considered in SSITU security architectures and 13315 is satisfied	C	
13310		Non-Functional Requirements	Ease of use, understandability and politeness	SPs need to enable SSITUs to carry out a high-quality incident response	SPs control large amounts of a SSITU system and so limit SSITUs' abilities to react	ESYS	Solutions offer SSITUs sufficient and timely information and access to enable them to react within GDPR's acceptable time-frames	C	
12210		Non-Functional Requirements	Cultural	Collectively the solutions available to SSITUs need to provide a realistic chance of security efficacy	SSITUs limit the perceived significance of risks that they think they can't reduce	LIT	The solution developed satisfies 10004 and 11142	C	
12213		Non-Functional Requirements	Ease of use, understandability and politeness	Solutions need to be implementable by unsupported SSITUs	11103, 11121	SSITU	Solutions are implementable by novices	C	
12214		Non-Functional Requirements	Ease of use, understandability and politeness	SSITUs need to use technology even when they have limited/ no computer literacy	11135	SSITU	Solutions are implementable by novices	C	
12221		Non-Functional Requirements	Learning and training	SSITUs need clear consistent advice	10007 and users losing self-efficacy due to conflicting advice	SSITU	Information related to the solution does not diverge from or contradict most prominent advice unless comparing solution efficacy; vocabulary used is consistent with most prominent advice	C	
12222		Non-Functional Requirements	Learning and training	The solution needs to promote SSITU self-efficacy	Price point precludes resource intensive support, inherent independence of entrepreneurs, 11105	ESYS	Solution implements all of 10005, 10006, 13317, and 13306	C	

RID	C	Reqt Category	Requirement type	Description	Rationale	Src	Fit	P	Conflicts
12224		Non-Functional Requirements	New problems and migration	The cyber security industry needs an accessible RA method for 'risk evaluator' SSITU group	Risk evaluator' SSITUs find existing RA process too cumbersome, but require evidence in support of cyber security investment	SSITU	There exists a RA process that's matches the time investment and formality of other SSITU risk evaluation practices	C	
13309		Non-Functional Requirements	Ease of use, understandability and politeness	SSITUs need low-key, easy to use, help in case of incident	Self-efficacy is lost post incident if a user is unsupported	LIT	Solutions provide enough support when something goes wring that 12222 is achieved	C	
13311		Non-Functional Requirements	Ease of use, understandability and politeness	Need something "cheap, quick and easy'' to deploy	10007, 12213	SSITU	Solution satisfies 11118 and is implementable by novice users	C	
13317		Non-Functional Requirements	Learning and training	SPs need to anticipate basic cyber security implementation support as part of services provided to SSITUs	SSITUs' most valuable assets are often controlled by SPs and are low-knowledge users who need to maintain self-efficacy	ESYS	Solutions offer cyber security specific support to their target user group	C	
12228		Non-Functional Requirements	Scalability or extensibility	SSITUs need security processes not to impede the immediate scalability of their IT systems	SSITUs use IT models that allow them to scale up/ down at short notice, possibly growing the system by more than 100%	SSITU	Solutions are of comparable flexibility to the systems they are protecting	C	
13308		Non-Functional Requirements	Cultural	SSITUs need security measures not to disrupt undocumented processes	SSITUs lack formalised documented processes, but their processes are critical to their operations	SSITU	Solutions do not suggest that SSITUs cease to carry out any activity, slow it down or require additional employees to complete	C	
13316		Non-Functional Requirements	Interfacing with adjacent systems	Need measures to adapt to 'legacy' processes	SSITUs' IT use evolves at low speed, especially where originally required high investment.	SSITU	Solutions do not suggest that SSITUs cease to carry out any activity, slow it down or require additional employees to complete	C	
13319		Non-Functional Requirements	New problems and migration	Security measures need to have no/low impact on SSITUs' operation	11136	SSITU	Solutions do not suggest that SSITUs cease to carry out any activity, slow it down or require additional employees to complete	C	
13320		Non-Functional Requirements	Reliability and availability	Need to maintain availability and reliability of IT system	11136	SSITU	Solutions do not measurably reduce the availability or reliability of the IT system in SSITU system use cases	C	
13301		Non-Functional Requirements	Access, integrity and privacy	SPs need to ensure that SSITU profiles/ identities are available and as intended	12240	SSITU	SPs maintain SSITUs' data in compliance with GDPR, even when the SSITU is a business rather than an individual	C	
13315		Non-Functional Requirements	Interfacing with adjacent systems	SSITUs need to be able to influence the quality of service they receive	12234 with 11130	ESYS	SPs take into account user requirements and make security a critical function when designing their service offerings	C	11129
13318		Non-Functional Requirements	Longevity	SSITUs need to have longer-term updates in high-investment devices (mobile phones etc.)	SSITUs lack the money to invest in new hardware when the old devices are still functional but unsupported	SSITU	Hardware solutions offer security updates that match the expected lifespan of the device's non-replaceable components	C	
12229		Non-Functional Requirements	Standards	SMEs need to benchmark against other SMEs	Incentive not to have a breach because they have failed to do wheat everyone knows you have to do	SSITU	Advice offered to SMEs gives a clear indication of what cyber security everyone else is doing	C	

RID	C	Reqt Category	Requirement type	Description	Rationale	Src	Fit	P	Conflicts
12230		Non-Functional Requirements	Standards	SSITUs need to prioritise protecting their reputation in their security architecture	11106	SSITU	Solution description highlights how it relates to the reduction of reputational risk	C	
12223		Non-Functional Requirements	Learning and training	SPs need to clearly communicate the solution's purpose in non-technical terms – is this a basic, reactive, or proactive reduction of risk? Is this intended to increase resilience?	SSITUs are low-knowledge IT users drowning in tech jargon but highly experienced in managing business risk.	SSITU	Novice users can understand the type of risk the solution is intended to reduce	I	
13303		Non-Functional Requirements	Access, integrity and privacy	SSITUs need suppliers not to be a threat to existing their cyber security/ privacy processes	SSITUs confound privacy and cyber security because personal privacy measures are reducing organisational reputational cyber security risks.	ESYS	Services offered to SSITUs must allow an opt-out of data collection or aggregation in line with data protection rules for individuals	I	
12205		Non-Functional Requirements	Cultural	SSITUs need more accessible case studies in advice offered or sales data	Known rather than unknown risks improve SSITU self-efficacy	SSITU	Information about the solution is offered in a format suitable for cyber security novices	O	
11118	AD	Design Constraints	Customer budgetary constraints	Budget of £10-50 per person per year in non-security-focussed SMEs, plus (where cost is hidden and service is reasonably priced) embedded security measures.	Reported by SMEs	SSITU	Overall cost of solution plus all other anticipated cyber security costs must be below this value	X	
11119	AD	Design Constraints	Customer budgetary constraints	Budget of £100-550 per person per year, up to a maximum of £10,000 for security focussed SMEs	Reported by SMEs	SSITU	Overall cost of solution plus all other anticipated cyber security costs must be below this value	X	
11120	AD	Design Constraints	Customer budgetary constraints	Not financially viable to have expert IT support/function for less than 25 employees.	Reported by SMEs	SSITU	Solutions are implementable by novices	X	
11121	AD	Design Constraints	Customer budgetary constraints	Not financially viable for a SSITU to have expert cyber security support/function.	Reported by SMEs	SSITU	Solutions are implementable by novices	X	
11122	AD	Design Constraints	Customer budgetary constraints	Lack of IT economies of scale	The difference between 11118 and 11119	SSITU	N/A	X	
11123	AD	Design Constraints	Customer budgetary constraints	Only organisations of more than 10 people have the capacity to begin considering secure configuration, access control, monitoring and user education.	Engagement reported by SSITUs compared to basic security advice	SSITU	N/A	X	
12238	AD	Design Constraints	Anticipated workplace environment	SSITUs favour security that has a transparent cost	SSITUs favour technical solutions with a 1-off and enumerable effort/cost	ESYS	Achieve 12206 and 12227	X	
12246	AD	Design Constraints	Current system environment	SSITUs favouring availability over confidentiality and resilience over pro-active security in decisions	Protecting continuity and favouring measures that have a clear return on investment	SP		X	
12250	AD	Design Constraints	Customer budgetary constraints	Cyber risks are not any more catastrophic than other risks for SSITUs	SSITUs favouring measures that have a clear return on investment. Cyber security is not achieving the same level of investment as comparable risks	SSITU		X	11142
14402	AD	Design Constraints	Customer budgetary constraints	SSITUs are constrained by the lack of resource and adaptability needed to support continual evolution		LIT		X	

RID	C	Reqt Category	Requirement type	Description	Rationale	Src	Fit	P	Conflicts
14401	AD	Non-Functional Requirements	Interfacing with adjacent systems	SSITUs need high-quality outsourced services to achieve adaptability in a sustainable way	12234, 11129, 14402	ESYS		C	11124, 11129
12206	AD	Non-Functional Requirements	Cultural	SPs need to enumerate the burden of security measures' configuration and use, and include this in their evaluation of acceptable price.	Underestimating the time or knowledge burden of implementing or using cyber security measures introduces a barrier to entry for SSITUs	ESYS	Overall cost of solution plus all other anticipated cyber security costs must be below 11119 or 11120	C	11104
12215	AD	Non-Functional Requirements	Ease of use, understandability and politeness	Solutions need to make impactful security decisions easy to adopt	SSITUs are choosing easy-to-implement technical cyber security measures over measures that required more effort but have greater benefits	SSITU	Solution offers sufficient evidence for SSITUs to differentiate it from alternative options and there is sufficient accessible advice for SSITUs to make risk-based decisions	C	11136
12226	AD	Non-Functional Requirements	Precision or accuracy	SSITUs need evidence-based solutions	12250, 12205	ESYS	Solutions are offered with advice on how to measure their efficacy and comparisons with other solutions or security architectures	C	11104
12227	AD	Non-Functional Requirements	Precision or accuracy	SSITUs need non-technical solutions to be enumerable/comparable against technical measures	12226	ESYS	Solutions are offered with advice on how to measure their efficacy and comparisons with other solutions or security architectures	C	11104

RID	C	Reqt Category	Requirement type	Description	Rationale	Src	Fit	P	Conflicts
20001		Project Drivers	Stakeholders	The project owner is a large RH, contracting a SP (who is likely to be another large organisation) to develop a solution	RHs experiencing sufficient risk to attempt to influence the supply chain	ESYS		X	
20002		Project Drivers	Stakeholders	The solution is Intended to be implemented by SSITUs, or across the supply chain, but the customer is undetermined.	RHs expecting the SSITU to pay to mitigate RHs' risks is a large contributor to the lack of supply chain security	ESYS		X	
20003		Non-Functional Requirements	Compliance	Stakeholders need clearer responsibility/ system transparency within the supply chain	Lack of transparency leaves gaps in responsibility that result in gaps in security	ESYS	Contracts clearly indicate system perimeters and stakeholder responsibility	C	
20004		Non-Functional Requirements	Cultural	Customers need not to be risky customers	Risky customers are finding services are withdrawn	SP	Customers achieve the benchmark for their type of organisation and do not present themselves as an easy or appealing target	I	11126
20005		Non-Functional Requirements	Interfacing with adjacent systems	RHs need to secure the supply chain to secure their larger organisations	21112, 21113, 21116	RH	RHs achieve 20006–20008, 21110, 21112-21115	C	21116
20006		Non-Functional Requirements	Interfacing with adjacent systems	Influential members of the supply chain need to increase the cost of SSITUs not engaging with *basic* security	While forcing SSITUs to reduce RHs risk has been unsuccessful, influencing the benchmark of 'basic' security expected of SSITUs and enforcing that is feasible	RH	SSITUs achieve Cyber Essentials or implement an equivalent level of security	C	
20007		Non-Functional Requirements	Interfacing with adjacent systems	SSITUs need influential members of the supply chain to cease to transfer unmitigable levels of risk to them	Transferred risk may be orders of magnitude higher value than the total assets of the SSITU	SSITU	RHs take SSITUs' abilities to absorb risk into account during their own risk assessments and achieve 20008	C	22210
20008		Non-Functional Requirements	Interfacing with adjacent systems	RHs need to have a better understanding of consequences and limitations of outsourcing when developing contracts	20007	ESYS	Contracts clearly reduce risk rather than just transferring it	C	11129, 11131
21109	OW	Project Drivers	Project purpose	RHs and SPs need to transition SSITUs from the bare essentials towards more advanced best practices to align their cyber security capability with other members of the supply chain.		ESYS		X	
21110		Non-Functional Requirements	Cultural	Supply chain security models need to accommodate the selection of small suppliers for contracts	21117	ESYS	Achieve 20005, 22206, 22208, 22212, 23304, 23305, and 23312	C	11121 + 20005
21111		Non-Functional Requirements	Cultural	SSITUs need larger stakeholders not to assume that lack of standards compliance/ equivalent practices means no security	Perceived lack of progress securing small organisations. SSITUs are making cyber security decisions that are relevant to the risk they face. Lack of action does not mean lack of awareness	ESYS	Solution uses the SSITU requirements framework to scope assumptions about SSITUs existing and potential capacity to implement security	C	
21112		Non-Functional Requirements	Interfacing with adjacent systems	RHs need interconnected systems for efficiency	Systems usually become interconnected at the request of a large stakeholder for their convenience	RH	Solution needs to allow systems to be connected	C	
21113		Non-Functional Requirements	Interfacing with adjacent systems	Stakeholders need interlinked services to increase reliability for their customers	IT-driven business model promotes an ecosystem of partnerships	RH	Solution needs to allow systems to be connected	C	

RID	C	Reqt Category	Requirement type	Description	Rationale	Src	Fit	P	Conflicts
21114		Non-Functional Requirements	Interfacing with adjacent systems	Contracts need to be satisfied across the supply chain	SSITUs are currently forced to accept risks instead of attempting to achieve contract KPIs because they can't achieve 23313 or 20007	ESYS	Achieve 23313 and 20007	C	20007, 21116
21115		Non-Functional Requirements	Interfacing with adjacent systems	Members of the supply chain need to protect customer confidence	If customer confidence is reduced so is service use, reducing all stakeholders' profits	RH/SP	Supply chain security solutions prioritise mitigating reputational risk	C	
21116		Design Constraints	Current system environment	Degrees of separation between between risk-holding and risk-influencing stakeholders, as well as contractual limitations, limit the ability to transfer responsibility with risk		RH		X	
21117		Design Constraints	Customer budgetary constraints	RHs need cost-effective or niche (and so often smaller) suppliers		RH		X	
21118		Design Constraints	Customer budgetary constraints	SSITUs can't afford to lose customers by disclosing breaches in order to ask for support, delaying RHs' incident response		SSITU		X	21114, 11132
22201		Non-Functional Requirements	Ease of use, understandability and politeness	The supply chain needs to develop a user friendly common vocabulary for SSITUs to communicate with experts within the supply chain	SSITUs are non-experts who conflate terms, but need to maintain their self-efficacy to be able to secure their organisations/ participate in supply chain security	ESYS	A common and consistent vocabulary is part of RHs' policy for interacting with their supply chain	I	
22202		Non-Functional Requirements	Immunity	SSITUs need to choose suppliers who offer enough ongoing support to avoid them losing incentive to employ secure practices	Low knowledge SSITUs often opt for fixed price services that exclude support, reducing quality of service	SSITU	Supply chain educates SSITUs about selecting suppliers	C	
22203		Non-Functional Requirements	Interfacing with adjacent systems	The supply chain needs SSITUs not to provide attack vectors that allow malicious actors to harm RHs	Suppliers as a vulnerability is the core motivation for RHs to attempt supply chain security	RH	The supply chain demonstrates a reduction in the security inequality of SSITUs in the supply chain	C	
22204		Non-Functional Requirements	Interfacing with adjacent systems	The supply chain needs to be able to identify the capability of threat actors	Likelihood of success depends on capability of attacker in relation to the capability of their target	ESYS	Contractual responsibility takes the capability of attackers into account so that risk is not transferred to stakeholders how lack the capability to mitigate	C	
22205		Non-Functional Requirements	Interfacing with adjacent systems	The supply chain needs to mitigate against the international nature of threats	Limited capability to attribute attacks and punish attackers increases attackers' incentive.	G	Larger stakeholders communicate with and influence government who have the capability to influence cross-border cyber security risk	C	11105
22206		Non-Functional Requirements	Interfacing with adjacent systems	Contracts need to differentiate between outsourcable mitigation requirements and untransferred risks	Mitigation requirements are well-scoped and of enumerable cost, risk is not.	ESYS	Contracts clearly indicate any specific technical stakeholder responsibilities	C	
22207		Non-Functional Requirements	Interfacing with adjacent systems	Supply chain security needs to independently identify the asset controller, asset owner and risk owner in interconnections to reduce the level of ambiguous responsibility	Shared/increased risk and responsibility	ESYS	Contracts including IT system interaction identify asset controllers, asset owners and risk owners for each identified risk	C	
22208		Non-Functional Requirements	Interfacing with adjacent systems	The supply chain needs to be able to articulate shared risk responsibility as a shared system requirement	The larger RHs have the capacity to engage with existing best practices	ESYS	Contracts take categories 2-5 into account when defining responsibilities, rather than focusing on category 1	C	

RID	C	Reqt Category	Requirement type	Description	Rationale	Src	Fit	P	Conflicts
22209		Non-Functional Requirements	Interfacing with adjacent systems	SSITUs need contracts to communicate non-functional security requirements, not uniquely tech-specific best practices	12247, 12248	SSITU	Contracts take category 2 into account when defining responsibilities.	C	
22210		Non-Functional Requirements	Interfacing with adjacent systems	RHs need to scope responsibility for risk across the supply chain to facilitate mitigation	Attackers only need 1 attack vector to succeed and SSITUs control some assets	ESYS	Contracts clearly indicate any stakeholder responsibilities	C	20007
22211		Non-Functional Requirements	Learning and training	SSITUs need large risk holders to consider supporting their supply chain partners as a valid mitigation	The risk being transferred to SSITUs is too large to mitigate against and 12222	ESYS	Contracts include an expert point of contact for SSITUs should they need security support	C	21118, 21117 – increases cost
22212		Non-Functional Requirements	Standards	SSITUs need large risk holders to influence large suppliers on their behalf	SSITUs lack the bandwidth to participate in the creation of standards and lack the influence to achieve favourable contracts	ESYS	RHs ask their representatives to educate themselves about SSITUs' needs and represent the supply chains' interests in workshops	C	11124
22213		Non-Functional Requirements	Standards	The supply chain needs to reduce the incentive for large organisations to retain/grow their control over consumer systems	12243	ESYS	RHs ask their representatives to educate themselves about SSITUs' needs and represent the supply chains' interests in workshops	C	11129
23301		Non-Functional Requirements	Audit and documentation	The supply chain needs to demonstrate the return on investment of reporting breaches to SSITUs	11105	SSITU	Breach reporting becomes a catalyst for SSITUs to receive 13309 and other risk owners gain visibility of potential threats	C	
23302		Non-Functional Requirements	Compliance	RHs need the ability to enforce security requirements across the supply chain	Unenforced requirements are not being addressed	RH	Contracts achieve 20007 and responsibilities are accompanied by the ability to question/audit services and consequences should the supplier fail an audit	C	
23303		Non-Functional Requirements	Cultural	SSITUs need supply-chain negotiating power	SSITUs are considered as consumers don't get to act as partners, impact of breach inevitably shared, fault-holder irrelevant except for goodwill	SSITU	RHs cease to consider SSITUs as 'price-takers' in the context of cyber security, allowing their capability to be taken into account in contracts	C	
23304		Non-Functional Requirements	Cultural	SSITUs need transparency from large RHs about their motivations to offer security support	Choices made across the supply chain need not to reduce SSITU trust in support offered	SSITU	Supply chain security is considered a partnership with the aims of the RH clearly stated	C	
23305		Non-Functional Requirements	Interfacing with adjacent systems	SSITUs need the supply chain to function as an ecosystem of partnerships	SSITUs need to have input into how supply chain security is approached	ESYS	Supply chain security is considered a partnership	C	
23306		Non-Functional Requirements	Interfacing with adjacent systems	Stakeholders need to assess how shared technical requirements can be implemented appropriately	Some technical requirements may be outside of the capability of SSITUs	ESYS	SSITUs allow RHs to implement/supply security measures on their behalf where they are outside of their capability and securing another stakeholder's risk	C	
23307		Non-Functional Requirements	Interfacing with adjacent systems	The supply chain needs system visibility and transparency to identify key stakeholders and assets	Complexity is an issue in identifying assets and dependencies	ESYS	23305 achieved and stakeholders supply information required for 23306	C	

RID	C	Reqt Category	Requirement type	Description	Rationale	Src	Fit	P	Conflicts
23308		Non-Functional Requirements	Learning and training	Supply chain may need to offer practical cyber security advice to SSITUs	12222	ESYS	Contracts include an expert point of contact for SSITUs should they need security advice	C	21118, 21117 – increases cost
23309		Non-Functional Requirements	Learning and training	Supply chain needs methods for supporting large numbers of SSITUs	23308 and 22211 make 21117 less affordable	RH	RHs work in partnership with SPs to support the SSITUs in their supply chain	C	
23310		Non-Functional Requirements	Learning and training	SSITUs need easy to access support to avoid 'support' being used as an attack vector	Self-efficacy and the sheer number of advice sources can lead to re-victimisation	RH/SP	Partnerships/contracts with SSITUs clearly define 'safe' sources of advice and support	C	21118
23311		Non-Functional Requirements	Standards	The supply chain needs to support SSITUs ability to employ behavioural mitigations to combat vulnerability to social engineering	Completeness of digital footprint	SSITU	Nothing requested of SSITUs increases their open-source digital footprint or reduces their ability to make privacy-conscious decisions	I	
23312		Non-Functional Requirements	Standards	The supply chain needs suppliers to allow SSITUs to terminate contracts when persistently poor cyber security practices are demonstrated	Suppliers who demonstrate a lack of due care and skill are taking advantage of their customers' 'consumer' or 'price-taker' status to only release those customers directly financially impacted to from contracts.	ESYS	Larger stakeholders communicate with and influence suppliers and ombudsmen	C	11129
23313		Non-Functional Requirements	Standards	Cloud services need to be more transparent about the quality of their security	SSITUs don't know what level of security their data is being held with	ESYS	SSITUs are able to get responses from suppliers about the quality of the security they offer at any point before or during a contract	C	