On Small-Scale IT Users' System Architectures and Cyber Security: A UK Case Study

Emma Osborn[a,*], Andrew Simpson[a]

[a]*Department of Computer Science, University of Oxford, Oxford OX1 3QD, UK*

Abstract

Despite long-standing predictions that developments in, for example, personal and cloud computing practices would change the ways in which we approach security, small-scale IT users (SSITUs) remain ill-served by existing cyber security practices. Following an extensive study of the adoption of cyber security in UK-based SSITUs, this paper discusses results pertaining to technologies employed by such organisations, with respect to their ability to apply security measures. We determine: that the system architectures employed by SSITUs are significantly different to those employed by large corporate or government entities; that 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 that 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; rather, there are additional needs to consider, including technology use in the context of interactions that occur within a broader ecosystem of a supply chain, users with multiple roles, and the impact of the digital footprint on security.

Keywords:
Cyber Security, Security Architecture, System Architecture, SME, Charity, Home Users, Supply Chain

1. Introduction

In the United Kingdom (UK), small companies (defined as employing fewer than 50 people) account for 99.3% of all private sector businesses and 48% of employment [1], 88% of charities in the UK (approximately 145,000) are also classed as micro, small or medium by the UK Charity Commission [2], and 92% of the population is online[1]. Despite this, small-scale IT users (SSITUs — defined in Section 2) do not typically spring to mind when one considers the term *cyber security*.

In 2011 the UK government released a National Cyber Security Strategy [3]. From the outset this mentions enhancing the security of consumers and smaller organisations as part of a broader aim to support economic growth. Of course, the need for cyber security in smaller organisations is by no means a new problem. In 1996, with the growth of personal computing, Carroll [4] wrote:

> "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." [4]

Unfortunately, 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"* [5]. 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 the measures that the UK government has identified as a minimum for reducing the risks they feel all UK Internet users face [6].

If attempts to increase the level of cyber security awareness in small organisations has not resulted in mitigated risks one might ask: *If a SSITU has justified investing in cyber security, what constraints within their IT system limit their decisions?* To this end, the paper focuses on system and cyber security architectures, drawing comparisons between the systems implemented and common corporate cyber security practices.

We report results of an empirical study that evaluated SSITU technology use, with respect to their ability to apply security measures, within a broader ecosystem of small-scale cyber security stakeholders in the UK. The study was motivated by a lack of available data about the environment in which these small organisations make their cyber security decisions, which makes the design of sector-specific security measures challenging.

The structure of the remainder of this paper is as follows. Section 2 describes the methodology used in the survey. Alongside the infrastructure (Section 3) and system interactions (Section 5) that make up a typical cyber security discussion, in Sec-

*Corresponding author
Email addresses: Emma.Osborn@cybersecurity.ox.ac.uk (Emma Osborn), Andrew.Simpson@cs.ox.ac.uk (Andrew Simpson)

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

tion 4 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 draw our conclusions in Section 6.

2. Methodology

The contributions of this paper, related to system architectures employed by SSITUs and the impact this has on their implementation of cyber security, emerged as part of a broader study into the security requirements of SSITUs [7]. The results we present are based on a *qualitative* empirical study, where a Grounded Theory approach was used to analyse data collected from two primary sources (similar to that employed by [8] or [9].)

The first dataset (collected using questionnaires and described in more detail in Section 2.2) focused uniquely on the security practices of SMEs (small to medium-sized enterprises). Although this dataset provided some insight into an under-researched user group, the less than 1% questionnaire response rate highlighted the difficulties in getting small business owners and directors to engage with research in this way.

As such, as well as expanding the scope of the study (as described in Section 2.1), our ability to interact with the user group and collect data has influenced project design and a second round of data collection. Recruiting participants in smaller numbers via interviews, engaging with them longer-term with periodic summaries of our results, and aiming towards a qualitative theoretical saturation (collecting data until new themes ceased to emerge, rather than reporting a quantitative statistical significance) have allowed us to create a meta-study of the sector, highlighting the key attributes of SSITUs' security practices.

2.1. Scoping and defining stakeholders

The initial SME dataset was first analysed independently of our new dataset. This initial study highlighted the importance of the interaction between SMEs and non-SME stakeholders in the ability for small companies to implement security [10] and led to our definition of stakeholders for the research we report here. We identify three (not mutually exclusive) stakeholder groups in the small-scale cyber security ecosystem:

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

Rather than focusing on the arbitrary definition of SMEs[2] as an example of a user group with different needs to those of the large corporate entities, we have expanded the scope to encompass a range of SSITUs. We consider SSITUs to be all entities without sufficient resources, infrastructure and requirements to warrant many of the measures advocated in the definitions of cyber security good practices [11, 12, 13] aimed at larger organisations. This group includes SMEs, start-ups, small charities or volunteer-run clubs, families and individuals.

The other stakeholder groups may not be SSITUs in their own right. However, the decisions they make, either due to the level of security they choose to embed in the products or services they provide, or by the need they express for smaller organisations in their supply chain to demonstrate security (and the actions taken to ensure this), may influence SSITUs' security capability. Some non-SSITU stakeholders, in particular law enforcement and professional membership organisations, were also able to give detailed descriptions of the technology used by SSITUs who had approached them for advice.

The first dataset consisted of 33 questionnaire responses[3], with 20 interviews in the second dataset (in line with the recommendations of Guest *et al.* that 12–20 interviews are the optimal number for developing significant results in a qualitative study [15].)

How our two datasets align to the stakeholder groups, as well as the proportion of stakeholders with low technical skill (LTS), is summarised in Table 1.

Data Source	**Number**	**LTS**
Questionnaire Data	33 SMEs	≈60%
Total interviews	20	45%
Interviews reporting on SSITUs	10	40%
Interviews reporting on SPs	12	58%
Interviews reporting on RHs	5	40%

Table 1: Participant statistics — the number of participants reporting from the perspective of each stakeholder group and the percentage with a low level of technical skill.

2.2. Data collection and analysis

The initial dataset was collected via a questionnaire, which attempted random sampling through mailing lists and social media. Statistics from that initial dataset (reproduced from [14]) are as follows:

- There were 33 respondents to the survey, 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.

[2] What is an SME? European Commission 2014: `ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/sme-definition/indexen.htm`

[3] Some results from this initial feasibility study can be found in [10], with a detailed description of the methodology and the questions asked in an extended technical report [14].

The second dataset was collected using detailed unstructured interviews with the stakeholders described in Section 2.1. Participants in 8 of the 20 interviews chose to talk about multiple organisations they were either involved in, or had interacted with in the supply chain. Sampling in this dataset was theoretical [16] — participants were recruited with the aim of increasing the number of themes within the dataset to provide a breadth of understanding.

We also made use of secondary sources, such as the Information Commissioner's monetary penalty notices[4], to enrich our results.

The results we report in this paper are the outcome of a Grounded Theory analysis, which Corbin and Strauss describe as an inductive process that *"builds theory from data"* [16]. The process begins with an area of study, allowing a theory to emerge from the data, rather than beginning with a hypothesis. This methodology was developed specifically for areas of research where there is limited knowledge of how a group of stakeholders' interactions influence an overall environment or goal. In some cases we use examples from our raw data to clarify our description of the themes that have emerged during our analysis.

3. System Architectures 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 [13]. 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* [17], the majority of which are still present in one form or another in contemporary standards and professional training (see, for example, [13] and [18]).

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 [17]:

- 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

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

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 2: Participant statistics — the number of participants reporting on each type of organisation architecture.

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 SSITUs implementing slightly different system architectures, with Sections 3.1–3.3 exploring the resulting IT infrastructure each type of SSITU maintains (this is complemented by a discussion on the virtual element of SSITU system architectures — the digital footprint — in Section 4). Table 2 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, rather than the purchase of preconfigured products — meaning that many SSITUs lack the time to acquire knowledge rather than being unable to afford basic security measures.

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 [19].

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.

3.1. 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 systems described by our participants and identified significant system differences dependent on organisational size.

3.1.1. Home architectures

The smallest of the SSITUs are individuals, in small home networks. At this stage the dataset already provides two distinct architectures: 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 architecture, generalised in Figure 1(a), is typified by a Small or Home Office (SOHO) router supplied by the user's internet service provider (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 architecture between 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).

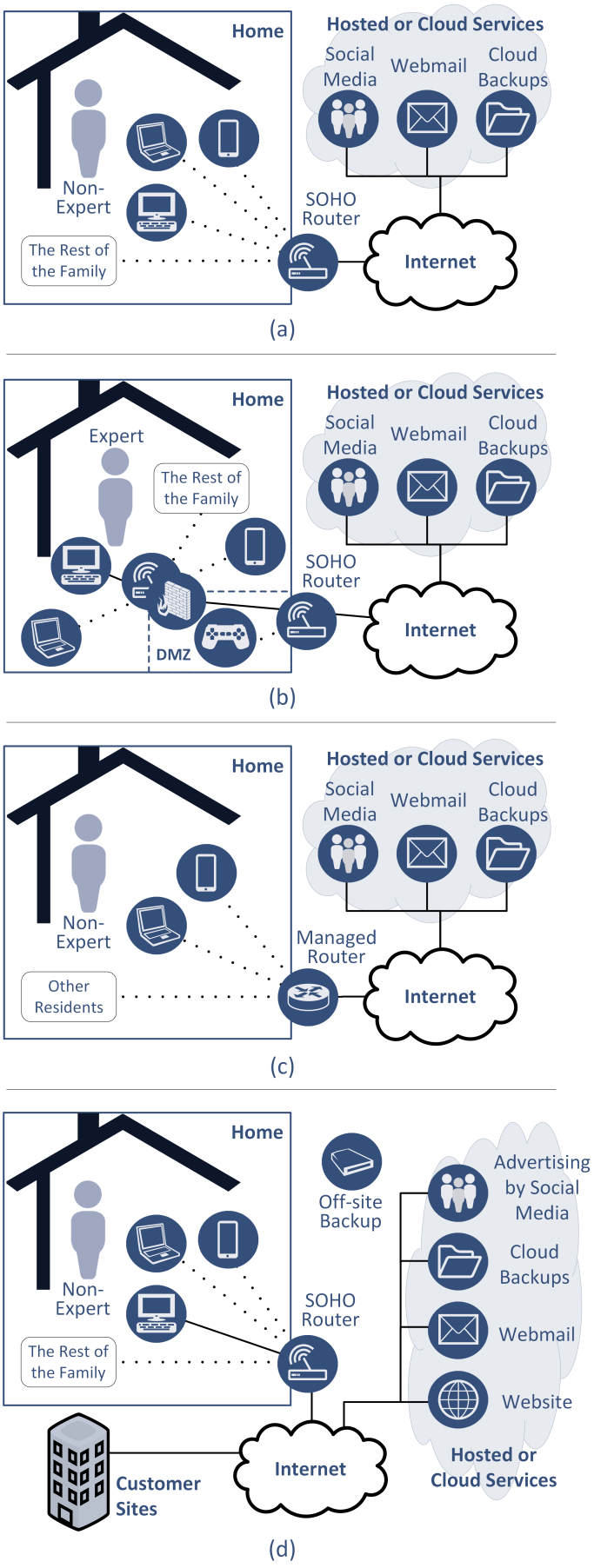


Figure 1: Home system architectures

- 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 1(b).

The second type of home architecture, generalised in Figure 1(c), is the architecture 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 architecture 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 architecture (Figure 1(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.

3.1.2. Single person companies

The UK Department of Business, Innovation and Skills Business Population Estimates for 2015 state that 76% of the 5.4 million businesses operating in the UK employ only the owner [1].

The first notable characteristic of single person companies is that most do not have dedicated offices. The participants working alone away from home 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.

In addition to the home architecture, these companies maintain a website and many have duplicate devices (typically smartphones or laptops) holding company data, of both the personal and work-designated varieties. The majority perform backups and use a variety of cloud services as well as employing basic security measures such as automatic updates and antivirus, irrespective of their industry sector or access to IT experts.

Half of our single person company participants have suppliers or customers who provide a link into their IT systems, or who they allow to link into theirs. The resulting network diagram (which, despite the addition of data, has not evolved since the original SME-focused study [10]) can be seen in Figure 1(d).

Comparing this architecture with the requirements of the UK government-endorsed Cyber Essentials Scheme [6], 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.)

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 1(c).

3.1.3. Micro-companies

The majority of micro-companies in our study (excluding the single person companies) had dedicated offices, although the least customer-facing industries (4 in our dataset — from the transport and software development sectors) were still able to avoid this expenditure.

There is an immediate difference in architecture 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 architecture described by this group of participants closer to that described in the scoping section of the Cyber Essentials Scheme documentation [6]. Two very different types of infrastructure emerged (Figure 2), but in both cases the size of the company means that they will still be able to use (questionably secure [20, 21, 22]) 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 3.3.

These companies all have websites, and there is a further increase in the number of devices per employee holding customer data. It is assumed that the increase in devices per person is due to a lack of a strict IT policy, rather than due to a higher requirement for multiple devices per person. These organisations described employing the same basic security measures as single person companies. However, there is a greater proportion of these organisations employing IT experts.

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

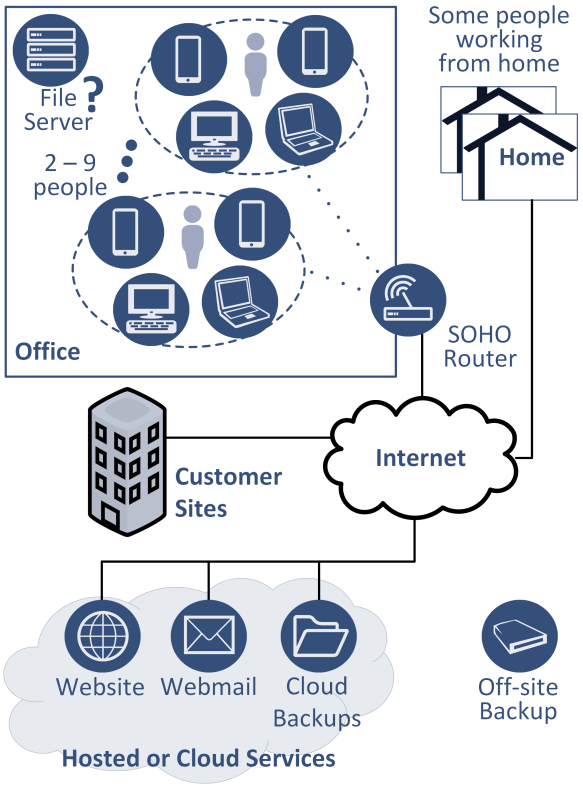


Figure 2: Micro-company system architectures

have a great impact on the hardware choices made by micro-companies. In the first architecture (Figure 2(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* [6].

The biggest difference between the two architectures is the number of SOHO-routed networks encompassed when employees are distributed in their homes, as can be seen in Figure 2(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 3.3 and Section 4 respectively.

3.1.4. Small and medium companies

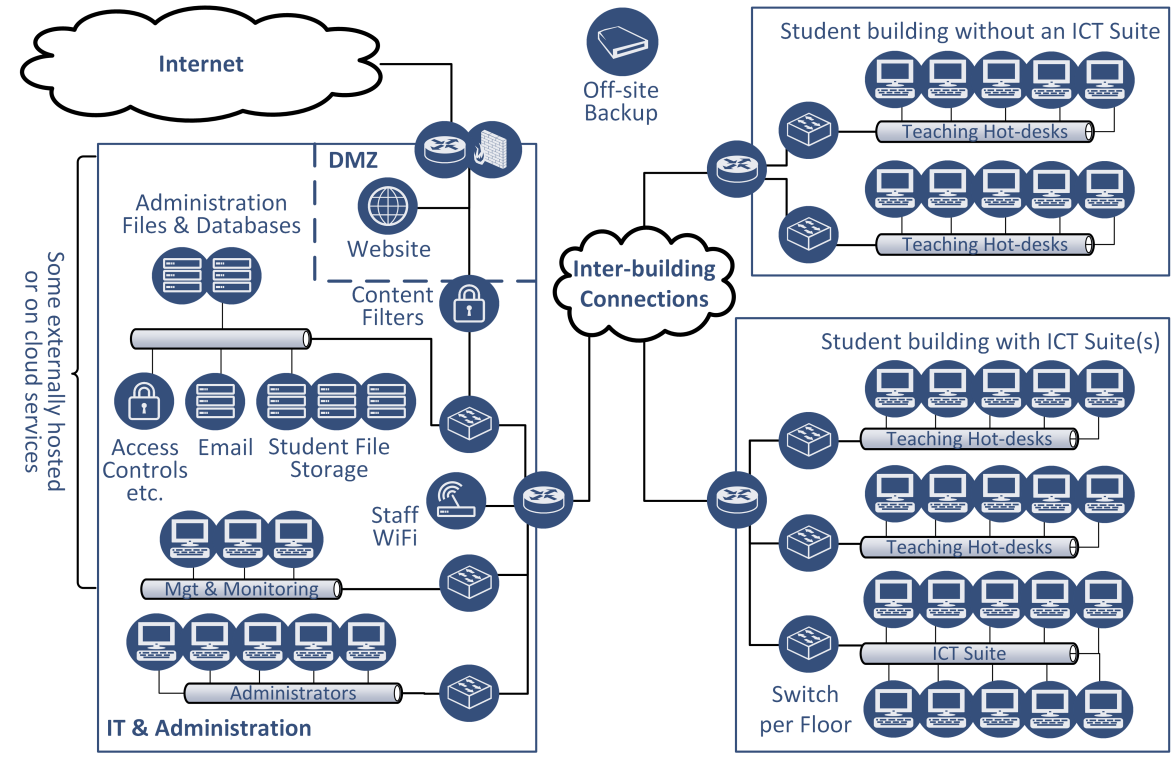
All of our participants working in companies consisting of between 10 and 249 people have dedicated offices. Companies where all staff are based in the same location are becoming too large to use SOHO routers — meaning that they are beginning to use elements of corporate IT network infrastructure. They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

Excluding some companies in the IT sector, companies of this size employ expert IT support, meaning that their architectures 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.

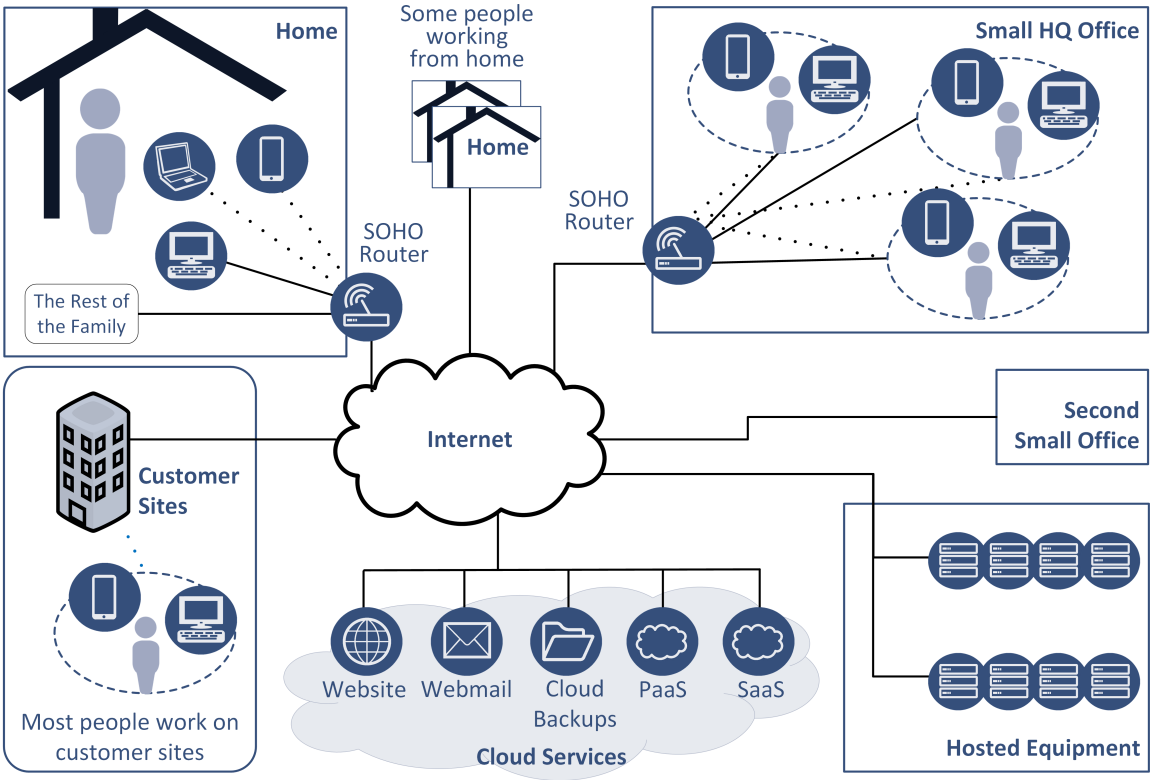
Our study indicates that companies of this size have sufficient control of their networks and devices, as well as the expert support required to focus on the elements of Cyber Essentials that smaller organisations typically struggle to achieve: *secure configuration* and *access control* [6]. Some of 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* [23] not included in Cyber Essentials: monitoring, incident response planning, and user education.

The smallest of these companies have limited differences in their system architecture when compared with those of the micro-companies, as illustrated in Figure 2. To show how infrastructures might evolve from this point, Figure 3 (which is reproduced from our initial SME-focused technical report [14]) 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 architecture appear more



(a)



(b)

Figure 3: Meduim-sized company system architectures

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 3.3.

3.2. Infrastructure by maturity

Not all small organisations are start-ups: 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 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 [24].

Mature companies are more likely than a start-up 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 architecture, potentially without clear ownership, and containing unsupported legacy equipment.

3.3. 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 3.1.4 and 3.2.

3.3.1. Low infrastructure organisations

A number of elements in the architecture 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 3(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 architecture advocated by some cloud researchers [25], 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 the large-scale measures employed by service providers should provide far better protection than the user can implement for themselves. A drawback is that these measures do not secure the user against the cloud provider itself — so the user has to comply with (and trust) the cloud provider's terms and conditions.

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.)

Some small organisations saw no reason to risk their data in the cloud. Where an organisation is large enough and sufficiently technology-centric it may become more cost-effective to retain in-house data centres.

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 the previous subsection 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 make up a key pillar of cyber security good practice [13] — 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 architectures 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 architecture. Start-up 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 3(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 to a PC[5]. As discussed in Section 3.1.4, at this scale this type of organisation can't be considered a SSITU.

[5] www.mountbatten.hants.sch.uk/home

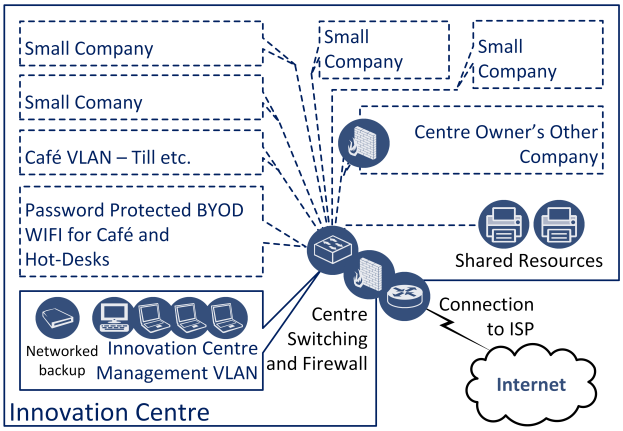


Figure 4: Innovation centre system architecture

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. Figure 4 shows one of these networks as described by the relevant participant.

3.3.2. Multi-purpose infrastructures

As discussed in preceding sections, the system architectures 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 the previous subsection, 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 implies the segregation of activities within a network so that appropriate access control measures can be applied [13, 6, 11]. 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 5 shows an example from our dataset of a home network used by both a family and single person company.

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.

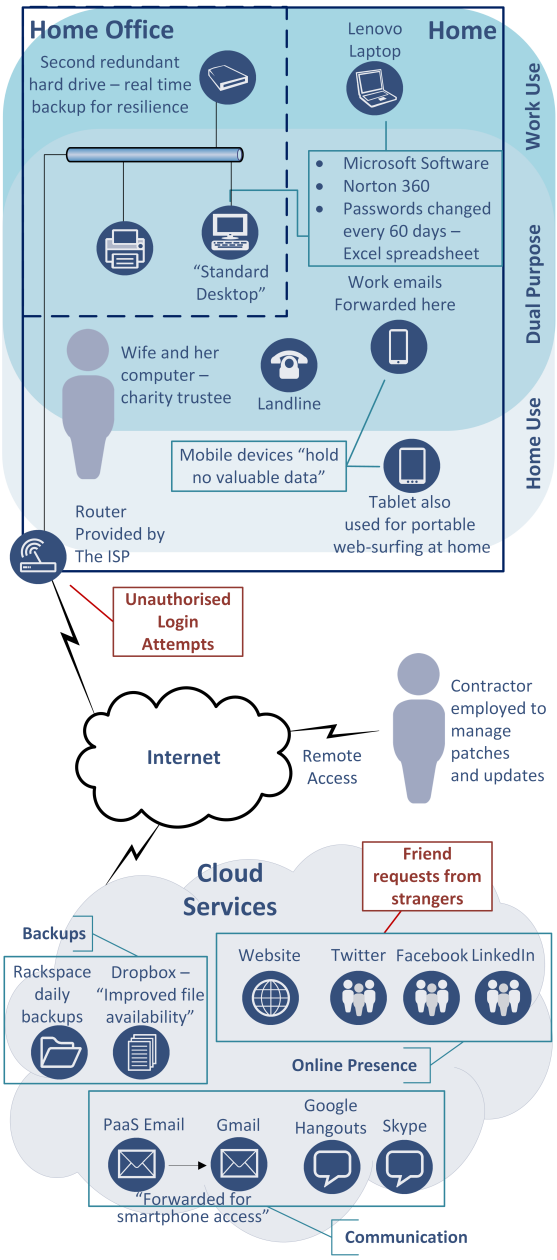


Figure 5: A multi-purpose home system architecture

- Start-ups 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.

3.4. 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 the previous subsection, 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.

Another issue highlighted for small organisations is mapping system architectures 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.

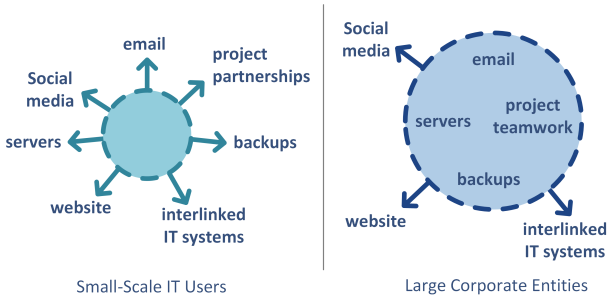


Figure 6: Abstract network diagram from an SME case study

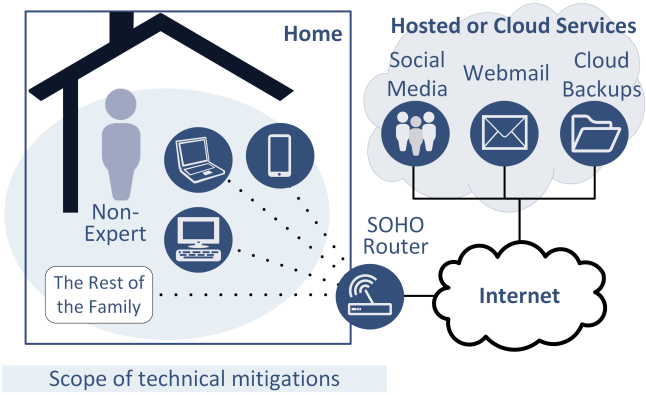


Figure 7: The available scope of cyber security mitigation considering only user-controlled technical system elements

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 6, 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.

An element of cyber security good practice involves managing investment in security measures to protect the most valuable assets [26]. 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 architectures described in this section are not best adapted to the defence-in-depth model described by [27], because they are unable to facilitate Carroll's principle to *"concentrate your valuable assets so they can be protected"* [17]. This means that for valuable

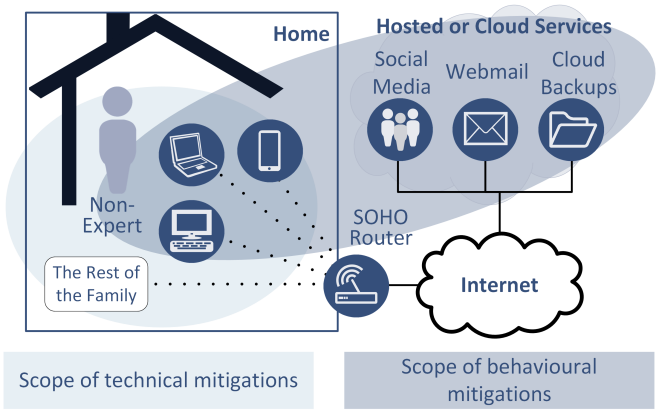


Figure 8: The available scope of cyber security mitigation when including behavioural mitigations within the digital footprint

items such as intellectual property small business owners are still relying on obscurity to keep their assets safe.

Security-providing 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.

Participants made decisions that favoured availability over confidentiality and favoured resilience over security in their businesses. In contrast home users limit or partition their service use to retain control of privacy and security.

SSITUs' knowledge is such that they find it difficult to avoid indiscriminate security measures: they often apply security measures without an understanding of product efficacy. A few participants with varying levels of knowledge described security fatigue. They made the choice not to worry: they reasoned that their security was equivalent to everyone else's, so their risk must also be acceptable.

Figure 7 illustrates how the scope within which SSITUs can mitigate security risks is limited by the system infrastructure they employ.

4. Interactions and the digital footprint

As we saw in the previous section, SSITUs have an increasingly complex online presence, with a significant portion of their systems existing in public cloud services. Larger organisations include intangible risks in a typical cyber security scope [28], 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

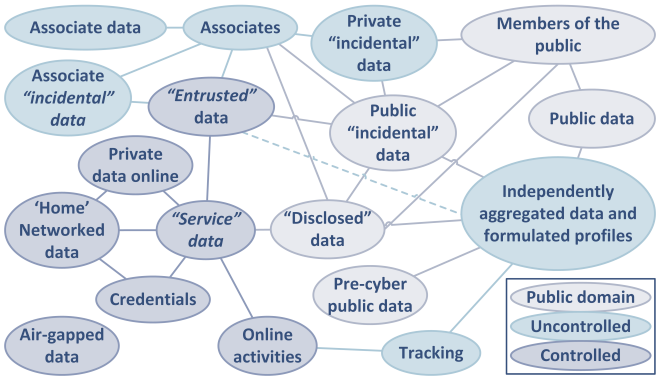


Figure 9: Digital footprint for a single user role

system, reducing intangible risk requires mitigating within the virtual element of the system. In Figure 8 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 3.

To this end, alongside the infrastructure (Section 3) and system interactions (Section 5) 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 different roles and third party decisions on elements of cyber security good practice, such as access control.

4.1. 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"* [29].

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 9 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* [30] 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 [31], positioning it within an environment in which a SSITU's reputation can develop.

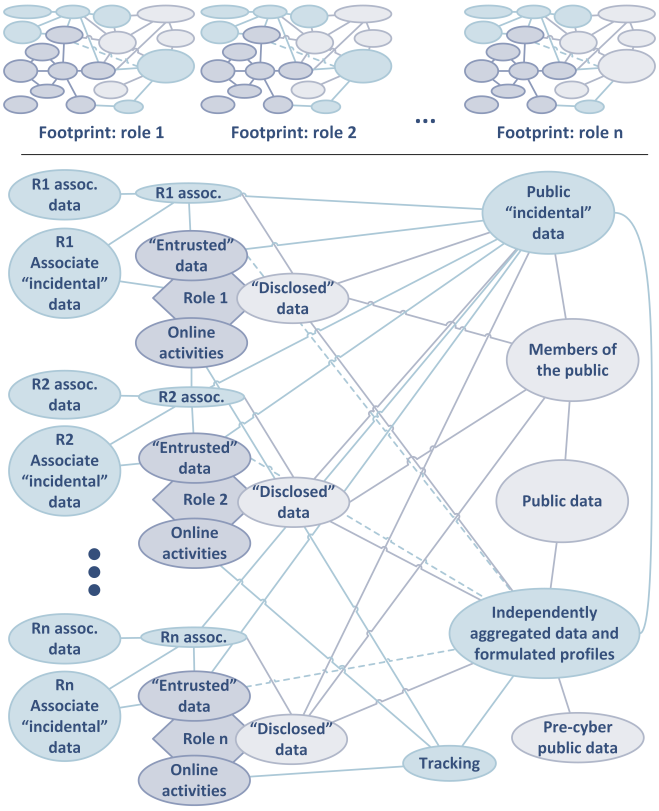


Figure 10: Digital footprint showing combined roles for a SSITU

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 9 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" [29] 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.

A digital footprint is made up both of a user's online activities and the digital artefacts produced by those activities [32]. 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 will contain both user-created and user-moderated (*active* [33]) content and unmoderated/uncontrolled (*passive* [33]) content, related or attributed to the user. In Figure 9 there is even a category of data (private contributions to data in online services) that the user has 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 10 shows, beginning to merge the footprints immediately introduces complexity into a user's

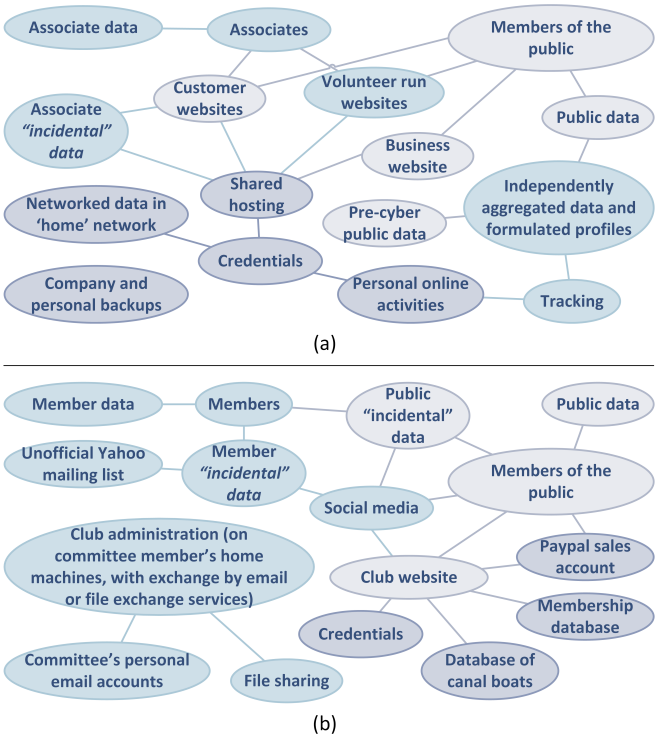


Figure 11: Example of an individual's and an organisation's digital footprints from a participant in our study

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 11(a).

As discussed in Section 3, 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 11(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.

4.2. *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." [29]

SSITUs 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 on the value they have to the user [26].

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[6]. 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[7].

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 [34]. This is an excellent way to retain customer interest and the connection they feel to the organisation, but

[6] www.bbc.co.uk/news/blogs-trending-35363394

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

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 pre-emptively 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 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: a certain amount of the digital footprint is out of the control of the subject [33]. 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 11(b) has chosen not to include a forum on their website. Instead, they have an unofficial mailing list on Yahoo, administrated 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 [35], 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 [35].

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." [29]

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.)." [29]

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.

4.2.1. 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. 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 [33]; 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 10 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 it is difficult (even as the data subject) to completely map a digital footprint [32].

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 [36, 37]; 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 [38] 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 unmoderated content [33].

Publicly available information is now more visible and has increasing impact and uncontrollable longevity, with harmful content having a longer lifespan [39]. 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[8], 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 [39]:

> "Old information threatens harsh and wide-reaching consequences to the socially valued and often protected individual interests of reputation, identity, and rehabilitation." [39]

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 [35]. This leads to the question, *when a data subject has no control over the creation of datasets does system or data control imply responsibility?*

[8] `www.google.co.uk/intl/en-GB/streetview/`

4.2.2. 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.

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 [40], force users to accept a certain level of business risk.

The example shown in Figure 11(a) shows the owner of a single person company and highlights the inseparability of the participant's personal and public profile. The multi-purpose infrastructures discussed in Section 3 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 compliance with data protection legislation [41]. 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" [42]. 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.

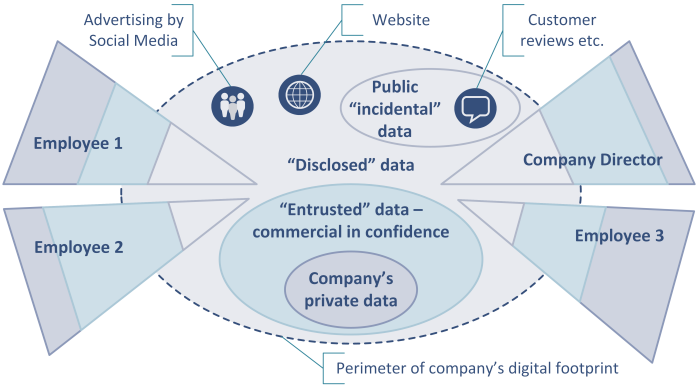


Figure 12: Example of how an organisation's digital footprint intersects with its employees'

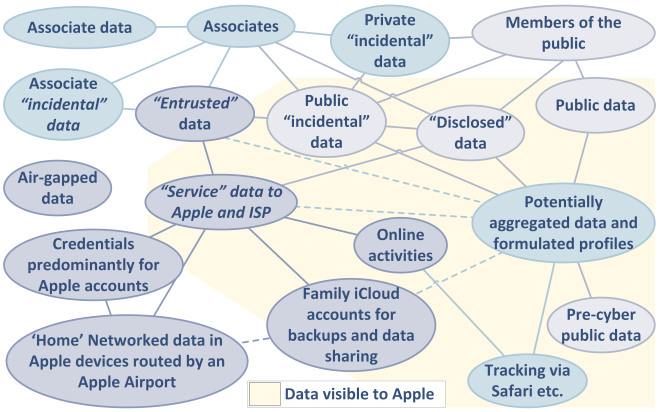


Figure 13: The digital footprint of a brand-loyal family

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.

4.2.3. Privacy-related decision making

In the context of this paper, 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 12. 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 [43]. 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 9). 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 data subject. The ability to deanonymise public datasets compounds the problem [44, 45, 46].

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.

Security is dependent on the attack surface that that user has created [47]; the difficulties SSITUs have in defining their system perimeter was described in Section 3. 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 13 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 [48]. 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.

4.2.4. 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.

4.3. 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 10. 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 11(a) and 11(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), 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 4.2 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. System interactions and interconnections in the supply chain

In Section 3 we discussed the different system architectures employed by SSITUs and the prevalence of multi-purpose infrastructures. In Section 4 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" [49].

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.

5.1. Supply chain complexity

All organisations are increasing their use of IT-driven service-based business models [50]. 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 [50]. Bartol suggests that, as a result of this complexity, a "defence in breadth" model is needed to secure the supply chain [51].

Complexity introduces a number of issues for cyber security good practice. One of our risk-holding 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 3, can reduce device function in a way that can limit security implementation. One security-providing 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 [52] the present authors discussed how these design complexities, instigated by the IT-driven business model [50], 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.

5.2. 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 be large organisations as other SSITUs.

All companies are making increasingly sophisticated use of technology, and this has led to modularisation, specialisation and division of labour [50]. 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 risk-holding participant indicated that this makes mapping the supply chain and its interdependencies (to evaluate risk) almost impossible for the end customer.

Vulnerabilities can be introduced at any point in a system life-cycle or the supply chain [51] — penalties issued by the UK Information Commissioner include breaches resulting from poor contracting of system transfers between old and new suppliers, as well as in development and implementation processes [53].

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 — it is no longer a simple choice to develop a system in-house due to the level of specialised knowledge required [50]. 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 risk-holding stakeholders, but there is still a need to measure the financial risks of contractor mistakes for security clauses in contracts to be enforced.

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 [54]. 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 small organisations have to operate at a higher level of risk than large organisations [40]. 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 risk-holding stakeholders of their varying risk appetites, which limits larger organisations' abilities to claim responsibility for risk they expect to have transferred.

5.2.1. 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 [55] and the good practice relating security measures to a cost-benefit analysis [26], 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 [56]. SSITUs may be benefiting from standards without incurring the expense of becoming accredited.

The UK government has developed a cyber security standard specifically adapted to include smaller organisations. Cyber Essentials attempts to define a benchmark for the minimum acceptable level of cyber security in any company that supplies the government, based on risks that the UK Technical Authority has identified as relevant for any Internet user [6]. 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 more 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 [55]. 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 outisde 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.

5.2.2. 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 [57] 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) [41].

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 [58]) 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 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[9]. SSITU interactions with service providers is discussed further in the following subsection.

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.

5.3. 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 1(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, customers of cloud services expect a supplier to hold some responsibility for security [59].

Negotiating power is related to size, meaning that small organisations are at a disadvantage when working with a larger organisation [40]. Unlike the SSITUs of Section 5.2, our participants were treated as consumers rather than partners even in business to business transactions.

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.

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

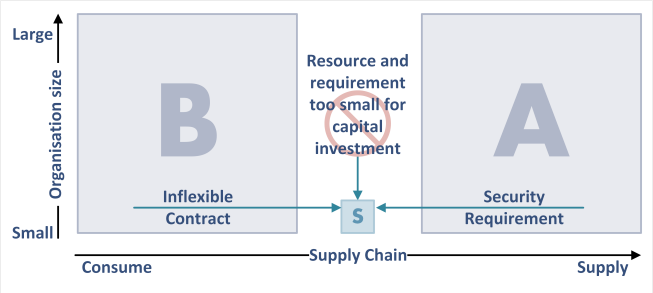


Figure 14: SSITUs in the supply chain

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 risk-holding stakeholders' opinion that SMEs in particular lacked security awareness. Due to the architectures described in Section 3 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 the IT-driven business model [50]. 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[10] 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. Distributing security

Sections 5.2 and 5.3 described constraints faced by SSITUs in interacting with larger organisations (as both customers and suppliers) to create the system architectures and accompanying digital footprints introduced earlier. These are summarised in Figure 14, 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.

[10]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`

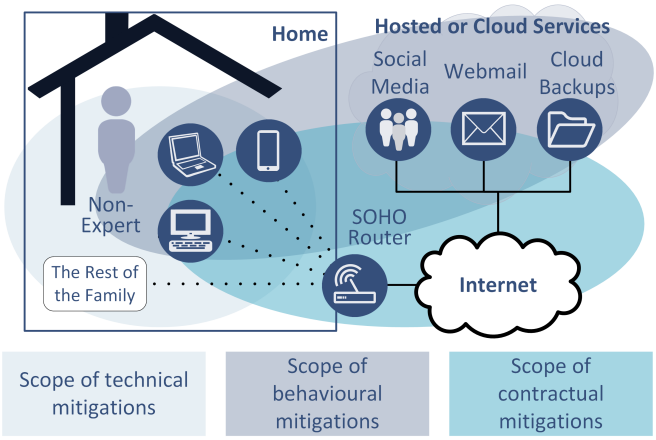


Figure 15: The available scope of cyber security mitigation when including contractual mitigations within the supply chain

Larger organisations, in the form of both risk-holding and security-providing 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 system architectures highlighted in Section 3, combined with the increased importance of managing their online activities discussed in Section 4, 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 14 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 [60]. However, the 'most influential' member of the supply chain may not be the risk-holding stakeholder — Egloff describes how technology companies are have become so large that they now assume "sovereign-like functions" [61] — risk-holding stakeholders may be unable to influence the decisions of the inadvertently security-providing 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 [62] and the characteristic low resources of SSITUs, will still limit results. We suggest that risk-holding 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 15, 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 [27].

6. Conclusions and Future Work

Having undertaken a survey pertaining to the cyber security requirements of UK-based SSITUs, we have evaluated the different manifestations of the differences between small-scale IT users (SSITUs) and larger government or corporate entities when it comes to the technology they employ and its impact on cyber security decision making. We have illustrated how, once a SSITU justifies the implementation of security, the choices they may make will be constrained by a broad number of limitations existent in the systems and community they operate within. These are as follows.

- System architectures for organisations under 10 people 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 systems that 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.
- Risk-holding stakeholders attempt to increase the security of SSITUs in the supply chain using standards to mitigate their own risk.
- Security-providing 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' [40] SSITUs experience insufficient flexibility in their interactions in the supply chain to influence overall security.

This paper shows that small-scale cyber security architectures are 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.

We intend to build upon these results. In a sister paper we evaluate how the reciprocal subject of cyber security risk and

business decision making is represented within our dataset, providing information on how SSITUs initially justify any investments in cyber security prior to implementation [63]. We intend to draw from these analyses to provide a set of attributes of SSITUs for a requirements framework, highlighting constraints and global requirements for this user group to facilitate product development in this sector.

7. Acknowledgements

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

[1] UK Government, Department for business innovation and skills business population estimates for the UK and regions 2015, www.gov.uk/government/statistics/business-population-estimates-2015 (2015).

[2] UK Government, Recent charity register statistics: Charity commission, www.gov.uk/government/publications/charity-register-statistics/recent-charity-register-statistics-charity-commission (2016).

[3] 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).

[4] J. Carroll, Computer Security 3rd ed., Butterworth-Heinemann, Newton, MA, 1996.

[5] 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).

[6] UK Government, Cyber essentials scheme: Requirements for basic technical protection from cyber attacks, www.gov.uk/government/publications/cyber-essentials-scheme-overview (2014).

[7] E. Osborn, A. Simpson, Small-scale cyber security, in: Proceedings of the 2nd International IEEE CSCloud Conference, IEEE, 2015, pp. 247–252.

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

[9] J. M. Ahrend, M. Jirotka, 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, pp. 1–10.

[10] E. Osborn, S. Creese, D. 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.

[11] ISO, Information technology — Security techniques — Code of practice for information security controls, International Standards organization, Geneva, Switzerland (2013).

[12] National Institute of Standards and Technology, Nist cybersecurity framework, https://www.nist.gov/document-3766 (2014).

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

[14] E. Osborn, Business versus technology: Sources of the perceived lack of cyber security in smes, ora.ox.ac.uk/objects/uuid:4363144b-5667-4fdd-8cd3-b8e35436107e (Sep 2014).

[15] G. Guest, A. Bunce, L. Johnson, How many interviews are enough? an experiment with data saturation and variability, Field Methods 18 (1).

[16] J. Corbin, A. Strauss, Basics of qualitative research: techniques and procedures for developing grounded theory, Sage, Los Angeles, 2008.

[17] J. Carroll, Computer Security 2nd ed., Butterworth-Heinemann, Newton, MA, 1987.

[18] ISO, Information technology — Security techniques — Overview and vocabulary, International Standards organization, Geneva, Switzerland (2016).

[19] D. R. Thomas, A. R. Beresford, A. 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, ACM, 2015, pp. 87–98.

[20] D. Pauli, Shodan boss finds 250,000 routers have common keys, www.theregister.co.uk (2015).

[21] C. Heffner, D. Yap, Security vulnerabilities in soho routers, www.exploit-db.com/docs/252.pdf (2009).

[22] M. Niemietz, J. Schwenk, Owning your home network: Router security revisited, in: Proceedings of the 9th Workshop on Web 2.0 Security and Privacy (W2SP) 2015, 2015.

[23] UK Government, 10 steps to cyber security, www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary (2015).

[24] D. Zissis, D. Lekkas, Addressing cloud computing security issues, Future Generation computer systems 28 (3) (2012) 583–592.

[25] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, I. Brandic, Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility, Future Generation computer systems 25 (6) (2009) 599–616.

[26] C. P. Pfleeger, S. L. Pfleeger, Security in Computing 4th ed., Prentice Hall, Boston, MA, 2007.

[27] Committee on National Security Systems, National information assurance (IA) glossary, www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf (2010).

[28] C. Alberts, A. Dorofee, Managing Information Security Risks: The OCTAVE Approach, Addison Wesley, Boston, MA, 2003.

[29] Oxford University Press, Oxford English Dictionary, Oxford University Press, Oxford, UK, 2016.

[30] B. Schneier, A taxonomy of social networking data, IEEE Security & Privacy 8 (4) (2010) 88.

[31] B. Wellman, J. Salaff, D. Dimitrova, L. Garton, M. Gulia, C. Haythornthwaite, Computer networks as social networks: Collaborative work, telework, and virtual community, Annual Review of Sociology 22 (1996) 213–238.

[32] S. D. Weaver, M. Gahegan, Constructing, visualizing, and analyzing a digital footprint, Geographical Review 97 (3).

[33] M. Madden, S. Fox, A. Smith, J. Vitak, Digital footprints — online identity management and search in the age of transparency, www.pewinternet.org/2007/12/16/digital-footprints (2007).

[34] Adaptly, Refinery29, 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).

[35] R. von Solms, J. van Niekerk, From information security to cyber security, Computers & Security 38 (2013) 97–102.

[36] H. Vandebosch, K. Van Cleemput, Defining cyberbullying: A qualitative research into the perceptions of youngsters, Cyberpsychology & Behaviour 11 (3).

[37] Y. Jewkes, Crime Online, Routledge, 2013.

[38] The World Bank, Internet users (per 100 people), data.worldbank.org (2015).

[39] M. L. Ambrose, It's about time: Privacy, information life cycles, and the right to be forgotten, Stanford Technology Law Review 16 (2012) 369–422.

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

[41] UK Government, Data protection act 1998, legislation.gov.uk (1998).

[42] M. 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) (2008) 662–674.

[43] K. Martin, R. E. Freeman, Some problems with employee monitoring, Journal of Business Ethics 43 (4) (2003) 353–361.

[44] A. Narayanan, V. Shmatikov, Robust de-anonymization of large sparse

datasets, in: Proceedings of the IEEE Symposium on Security and Privacy, 2008, pp. 111–125.
[45] P. Ohm, Broken promises of privacy: Responding to the surprising failure of anonymization, in: University of Colorado Law Legal Studies Research Paper, University of Colorado Law School, 2009, pp. 09–12.
[46] G. Wondracek, T. Holz, E. Kirda, C. Kruegel, A practical attack to deanonymize social network users, in: In Proceedings of the 2010 IEEE Symposium on Security and Privacy, 2010, pp. 223–238.
[47] P. K. Manadhata, J. M. Wing, An attack surface metric, IEEE Transactions on Software Engineering 37 (3) (2011) 371–386.
[48] J. W. Jerome, Buying and selling privacy: Big data's different burdens and benefits, Stanford Law Review Online 66 (2013) 47.
[49] K. W. Miller, J. M. Voas, G. F. Hurlburt, Byod: Security and privacy considerations., It Professional 14 (5) (2012) 53–55.
[50] H. Kagermann, H. Osterle, J. M. Jordan, IT-driven Business Models: Global Case Studies in Transformation, Wiley, 2010.
[51] N. Bartol, Cyber supply chain security practices DNA – Filling in the puzzle using a diverse set of disciplines, Technovation 34 (7) (2014) 354–361.
[52] E. Osborn, A. Simpson, On safety and security requirements in emerging ubiquitous computing models, The Computer Journal 59 (4) (2016) 570–591.
[53] Information Commissioner's Office, Action we've taken, `ico.org.uk/action-weve-taken/` (2015).
[54] J. Ritter, Achieving digital trust: new rules for business at the speed of light, Self-published, USA, 2015.
[55] ISO, Information technology — Security techniques — Information security risk management, International Standards organization, Geneva, Switzerland (2011).
[56] E. Yeniman Yildirim, G. Akalp, S. Aytac, N. Bayram, Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey, International Journal of Information Management 31 (4) (2011) 360–365.
[57] UK Police, Action Fraud - national fraud and cyber crime reporting centre, www.actionfraud.police.uk/ (2016).
[58] CERT-UK, Cyber-security information sharing partnership (CiSP), www.cert.gov.uk/cisp (2016).
[59] L. M. Kaufman, Data security in the world of cloud computing, IEEE Security & Privacy 7 (4) (2009) 61–64.
[60] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications 34 (1) (2011) 1–11.
[61] F. Egloff, Cybersecurity and the age of privateering: A historical analogy, Cyber Studies Working Papers 1.
[62] N. G. Leveson, Safeware: System Safety and Computers, ACM, New York, New York, USA, 1995.
[63] E. Osborn, A. Simpson, Risk and the small-scale cyber security decision making dialogue — a uk case study, Submitted for review by The Computer Journal.