UNIVERSITY OF OXFORD

CENTRE for DOCTORAL TRAINING in CYBER SECURITY

CDT Technical Paper

01/15

Business versus Technology: Sources of the Perceived Lack of Cyber Security in SMEs

Emma Osborn

Business versus Technology: Sources of the Perceived Lack of Cyber Security in SMEs

Emma Osborn
University of Oxford
Centre for Doctoral Training in Cyber Security
emma.osborn@cybersecurity.ox.ac.uk

September 2014

Keywords: SME; requirements; barriers; Cyber Security

There is increasing concern about the standard of cyber security in SMEs, voiced by governments and the large companies who interface with them, yet many past initiatives seem to have failed to have a significant impact on the sector. In this paper, we report upon a study in which Small and Medium Enterprises (SMEs) were surveyed to establish what barriers they might face in terms of cyber security. The results were combined with publicly available information to identify how stakeholders in the SME cyber security ecosystem interact, and establish whether the perceived lack of uptake of cyber security measures in SMEs was accurate. The paper concludes by discussing how the refined understanding of the barriers faced by SMEs might influence development of future SME security solutions.

1 Introduction

The European Commission states that 99% of businesses in Europe are Small and Medium Enterprises (SMEs), using the definition provided in EU law (EU recommendation 2003/361 [1, 2]), which can be seen in Table 1. This defintion is used in the UK where SMEs accounted for 59.3% of private sector employment and 48.1% of turnover in 2013 [3].

Despite this products, standards and the education of cyber security professionals most often focus on big budget options for securing large organisations. While the threat and implications of a cyber security incident are considered higher in large organisations, a lack of downwardly scalable and affordable options for SMEs may, through volume of small incidents and inability to meet standards, put these businesses and the wider supply chain at risk.

While there are risks posed by the way SMEs are perceived as approaching cyber security, the sector also represents a huge marketplace for any supplier able to produce suitable user-friendly and low cost solutions. Currently only antivirus products have become widely adopted in the sector, which raises the question why comparatively few companies have managed to make the business case for developing with this sector in mind; or why SMEs appear to be so much slower in adopting the products available to them than larger companies and government?

Company Category	Employees	Turnover or Balance Sheet
Medium-sized	<250	≤ €50m or ≤ €43m
Small	<50	≤ €10m or ≤ €10m
Micro	<10	≤ €2m or ≤ €2m

Table 1 EU SME Definition

This study began by approaching SMEs to get their perspective on cyber security issues. A questionnaire was developed and presented to SMEs, details of which can be found in Section 2, asking SMEs about their security behaviours and requirements. Information from the questionnaire has been combined with publicly available information about how other government and private sector stakeholders influence the SME cyber security marketplace, in order to describe the often disjointed dialogue between the stakeholders in this ecosystem, and its outcomes.

The point of view of each stakeholder group is described in Sections 3.1—3.3, focusing on the phenomenon that best describes the perspective of that group on the SME cyber security problem. Section 6 concludes the paper, discussing outcomes, lessons learned, and possible directions for future work.

To aid the reader some high level statistics about the questionnaire dataset are outlined in the following subsection.

1.1 Questionnaire Statistics

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 Methodology

2.1 Data Collection

2.1.1 The Questionnaire

The primary source of data for this study was a questionnaire, aimed at SME owners, directors or managers and consisting of 19 questions or questions sets. Full details of the questions asked can be seen in Annexe A.

A questionnaire was considered the best way to collect a coherent set of results, while working within the time constraints faced by SME directors. Participants were given additional contact details, to allow those who had more time and wished to continue interacting with the researcher the chance to express their interest.

The questions covered seven themes:

- Basic metrics about the company.
- The size of the company.
- The company's technology use and budgets.
- The respondent's cyber security knowledge and awareness.
- Details of the cyber security risks held by the company.
- Behaviour within the company and current cyber security measures.
- The company's high level cyber security requirements.

The questions were developed by the researcher based on her knowledge of the cyber security and SME sectors, peer-reviewed, and piloted by two SMEs working with Oxford University as cyber security industry partners. The questions were also reviewed by an SME director in the accountancy sector, to ensure their accessibility to non cyber security experts.

To introduce an extra level of granularity, an extra category of SMEs was defined in the response ranges of these questions – companies which had only one person. The reason for this is that there is a significant difference in business process between a micro company and a person who works for themself. To align the turnover question with the number of people an extra financial threshold was defined using the current UK VAT threshold, the intention being that this value would be independently re-calculated over time, so that the thresholds maintain the same significance.

2.1.2 Other Data Sources

Questionnaire data was combined with information from three other sources:

- Observations about the functionality of SME websites and insight into cyber security awareness gained during the data collection process.
- Additional information respondents have requested be added to the dataset by contacting the researcher directly.
- Literature available about SME cyber security surveys, incentives, initiatives, and the SME security marketplace.

2.2 Participant Selection

There are around 4.9 million SMEs in the UK [3], so a means of sampling a cross section of the community had to be defined for this project. It was felt that to show a representative cross-section, respondents had to be from different sized companies, in a variety of industry sectors and not all from the same county, where a specific initiative may have been run.

In order to obtain this cross-section a variety of means were used to identify potential respondents – the researcher's professional contact list, Oxford University

social media accounts and by using council local business directories to locate websites or email addresses. Respondents were then contacted by email.

The questionnaire was aimed at the owners, directors or managers of SMEs. The first question in the survey was the respondent's role, which when combined with the company size question can prove whether responses were from the targeted audience. The majority of respondents were managers, owners or company directors and all respondents were from SMEs.

2.3 The Dataset

2.3.1 Limitations

The scope of the model is limited by the number of survey responses received. Only 33 responses are included in the dataset.

2.3.2 Selection Biases

There was no financial incentive for SMEs to participate in this research, as such there will be an abnormally high number of respondents who indicated that they know what cyber security is, and feel that it is important. This selection bias was unavoidable, as people with no interest were unlikely to engage with us.

Almost all respondents had their own website. Consultation with an SME industrial partner suggests this is realistic, as having a website is becoming a necessary means for companies to prove their credibility. However, given that a large proportion of respondents were contacted via contact details on their websites, the participant selection method has potentially skewed the data.

To obtain a cross-section of SMEs which included some who do not know any cyber security professionals, and which covered industry sectors beyond those in the researcher's contact list, companies had to be contacted who had never spoken to the researcher before. This collection method may have produced a selection bias towards respondents with a low level of cyber security awareness, as it is widely accepted as poor cyber security practice to follow a link in an unsolicited email. A small number of respondents did email the researcher to question this before clicking on the link.

A small proportion of respondents were not company directors or owners. In those cases the data was included in the dataset, but care was taken to establish that the responses were not outliers to the dataset which could indicate a lack of accuracy in responses.

Respondents are far more likely to come from a micro or small company than a medium one. This is a representative section of the business community where micro companies vastly outnumber medium-sized companies, however the participant selection method collected mainly 'info@' addresses from company websites. In the larger companies this would mean that the email was reaching a sales or support team rather than a company director.

2.3.3 Methods of Analysis

A large proportion of the dataset could be numerically coded, meaning that where possible basic statistical measures were used to establish dependence of a response against one or more explanatory responses [4].

Every response in the dataset which could be numerically coded was treated individually as a dependent y-value. Multiple linear regression was used against the whole numerically-coded portion of the dataset, with the explanatory x-values of company size, industry sector, dedicated offices, various combinations of different cyber security risks, and responses grouped to indicate use of cloud services or basic awareness. X-values which resulted in an adjusted R^2 value greater than or equal to 0.3 were considered to influence the response to the y-value. There were no adjusted R^2 values greater than 0.7. Adjusted R^2 values between 0.2 and 0.3 were used to indicate where there may be some relation between x and y-values so that that section of the dataset could be manually investigated.

Y-values which had no clear relation to any of the x-value groups used were investigated further, and fell into two categories – those where no pattern could be found in the numerically coded data, and questions where the response was close to unanimous. In the case of close to unanimous results the outliers were identified for further analysis.

The significant adjusted R^2 values, identified outliers and some sets of manually investigated data where patterns could be explained by open response questions were open coded, along with the open response questions, observational and literary data, to form the basis of a Grounded Theory based set of concepts [5].

Concepts were axially coded to form categories which described the context and relating actions and consequences of each identified phenomenon, the categories

eventually forming an identifiable hierarchy which led to the identification of an emerging theory, which is described in Section 3.

The draft version of the theory was presented in detail to two SMEs in order to gauge the accuracy of the data analysis, with a few minor adjustments being made to arrive at the model presented in this paper.

3 The Perceived Lack of Uptake of Cyber Security Measures in SMEs

The model described in this section, characterising the SME cyber security ecosystem, is the result of the application of grounded theory, and can be succinctly described as *the perceived lack of uptake of cyber security measures in SMEs*. The intention is to highlight the impact of the disjointed dialogue between the three main stakeholder groups in the ecosystem.

The point of view of each group is described in subsections 3.1 – 3.3, focusing on the phenomenon that best describes the perspective of that group on the SME cyber security problem. These phenomena are combined with the relevant survey results and literature to show at each point how SME stakeholders are interacting in response to a phenomenon. Membership of the stakeholder groups is also not mutually exclusive – an SME can be in the cyber security sector and concerned about SME security.

3.1 Concerns Over Cyber Security in SMEs

This subsection focuses on the stakeholders within the SME cyber security ecosystem who are voicing concern over the level of cyber security achieved by SMEs. Cyber security in SMEs is an issue which seems to periodically cycle in and out of the spotlight.

There are three main arguments given for concern over SME cyber security:

1. The suggestion that SMEs are being used as attack vectors for large companies or government departments higher up the supply chain [6].

2. Attacks reported by SMEs in surveys such as the UK Department for Business Innovation and Skills (BIS) Information Security Breaches Survey [7].

3. The political moral incentive – the risk of financial loss from cyber incidents versus the number of SMEs in the UK, the percentage of the GDP they account for and the amount of employment they provide [8].

The concerns stated above have been the drivers for various SME security initiatives, and the issues gain more press attention at the times when they are being paired with the announcement of a new initiative to improve SME security.

Past initiatives include ENISA's Risk Assessment and Risk Management Methods: Information Packages for SMEs (March 2006) [9] and ISSA-UK's Security Standard for SMEs (March 2011) [10]. The ISSA standard reported in the article cited here cannot currently be accessed, so no evaluation can be made of its content in comparison to current initiatives. The ENISA information package is still available and, while some of the advice it contains now seems fairly dated in the face of emerging attacks, it does describe a risk analysis process in accessible language. The issue is with the way the advice is framed as business processes, audits and with only high infrastructure organisations given in the case studies – a scenario a large percentage of SMEs would have trouble identifying with.

Present UK government initiatives are slightly more varied in their approaches and development process: the Cyber Security Voucher Scheme, Cyber Streetwise and Cyber Essentials [11, 12, 13]. All of these initiatives were launched recently, so it is difficult to gauge the success of any particular approach at this time. SMEs being heavily involved in the development process may have focused the content sufficiently to better engage the target audience. There are also initiatives in the private sector, from professional membership groups providing information about cyber security to SMEs such as IASME developing standards specifically adapted to smaller organisations [14, 15, 16].

Large numbers of stakeholders, including some SMEs themselves, are voicing concern over cyber security issues. When combined with visible investment in initiatives aimed at alleviating the problem, this should theoretically have led to secure SMEs, so one may ask where are the barriers?

3.1.1 Concern 1

Full details of attacks are rarely published, meaning that concern 1 could be viewed as hearsay, but even with

concrete and SME-accessible evidence that this is the case, the risk owners are not the SMEs. The SMEs surveyed in this study were asked whether there was a risk of them losing business due to customers asking them to adhere to cyber security standards. Respondents were almost unanimous in emphatically denying any pressure having been put on them by the supply chain – risk is not being systematically transferred.

There are two outliers, the first of which is an education establishment that is in the medium size company bracket. This company has its own dedicated offices, and is large enough that the respondent holds the role of IT director. It is therefore thought that this company has more fixed infrastructure than any other participant in the survey, making them behave more like a large company. Further justification for this is outlined in Section 3.2.1.

The second outlier was the only respondent in the manufacturing sector – a sector which is already heavily standards reliant and far more likely to be part of a government supply chain. A high percentage of SMEs have their main customer base in the SME or home marketplaces where there would be less pressure from the supply chain.

3.1.2 Concern 2

Unlike concern 1, concern 2 could directly impact an SME's profitability, however in the BIS survey [7] the respondents were mainly from much larger companies, with only one in three not holding an IT or security role. As discussed in Section 2.3.2 respondents in this study are far more likely to come from a micro company. The BIS survey participants self-select, so it is probable that responses come from the people personally interested in the answers the survey provides, accounting for the large number of IT and security staff.

In this study survey respondents were asked if their companies had dedicated IT support staff to set up their computers. Only 16 participants said they had IT staff, these 16 falling into two groups – companies large enough to have a separately defined IT function, and those smaller companies who are in sectors where their chargeable hourly rate is greater than or equal to the hourly cost of the IT professional they could outsource to. For the group of companies without an owner/director personally interested in cyber security, choosing to find, read and believe the survey would cost a company money, so there is no incentive to seek this information.

The survey asked participants to rate their agreement with the statements *"I don't know what cyber security is"* and *"I don't care what cyber security is"*. Within the respondent group there were four who admitted they did not know, or were not sure what cyber security was, but there was only one who said they did not care. There were two further questions aimed at establishing where any concerns they might have were from, and in both cases the responses were mixed.

The press would be responsible for enabling cyber security statistics to reach outside of the IT and security sectors, but only 36% of respondents had some agreement with the statement that the press had made them worried about cyber security. 60% of respondents either agreed or strongly agreed that someone they knew had made them think cyber security was important. It is clear from these results that the people within a company director's social network are for more influential than the problem being widely publicised.

There were four respondents who disagreed or strongly disagreed to both being influenced by acquaintances and the press. None of these respondents stated they they did not know or care what cyber security is, so these two influences alone do not account for all sources of concern within the SME sector. Respondents to this study's survey gave no specific indication that the source of their concern was having previously experienced cyber attack.

3.1.3 Concern 3

Concern 3 is a political argument, the risk holder being UK PLC. Moral incentives of this type are documented as being poor motivators due to the underlying message that nobody is achieving what they are expected to [17], but SME owners and directors also typically have a different attitude when it comes to their companies than the average employee. People who have chosen to start a company because they want the freedom of working for themselves would probably interpret this argument for cyber security as unwelcome and unwarranted government interference.

While a level of support for SMEs wanting to implement cyber security exists, the incentives supplied to SMEs are not as well evolved. What is largely driving concern and the resulting development of cyber security initiatives are risks and requirements owned by *large* organisations.

3.1.4 The Impact of the ICO on Concern About SME Security

The arguments for concern discussed in the preceding three subsections all attempt to offer an incentive for SMEs to improve their cyber security. The Information Commissioner's Office (ICO) is different, firstly because in this case the arguments and incentives are not aimed at protecting SMEs; rather, the aim is to protect the general public from any organisations being less than careful with the personal data they hold.

The second reason the ICO is different is that they are offering a clear negative incentive – the argument for cyber security is not that SMEs need cyber security to protect their profitability, or the UK economy. The ICO defines clear financial and reputational penalties for any organisation found to be leaking personal data. The very high proportion of respondents aware of their data risk may be linked to the success in publicising the ICO's negative incentives.

The survey asked respondents if they agreed with the statement "We have customer or supplier data that we need to protect". 82% agreed or strongly agreed with this. The impact of this, along with the other risks respondents were asked about, are discussed in Section 3.3.

3.2 Lack of Cyber Security Industry Focus on SMEs

The cyber security industry has developed over time in response to risks posed by cyber threats, with government and large companies leading they way as they have both represented the most lucrative target and are the sectors most able to finance the development of cyber defences. Cyber security measures are derived from the identification of vulnerabilities, with solutions ranging from software patches, to security specific tools, specialist staff and business processes.

If the funding, or potential purchasing power, needed for the development of cyber security measures comes from government and large industry, it is within government and large industry style infrastructures that vulnerability researchers will search for problems. This raises the question of scalability – to what extent do these solutions apply to smaller organisations?

Some of the building blocks that make up these infrastructures are almost identical to those used in the home, typically at the network endpoint. In these cases

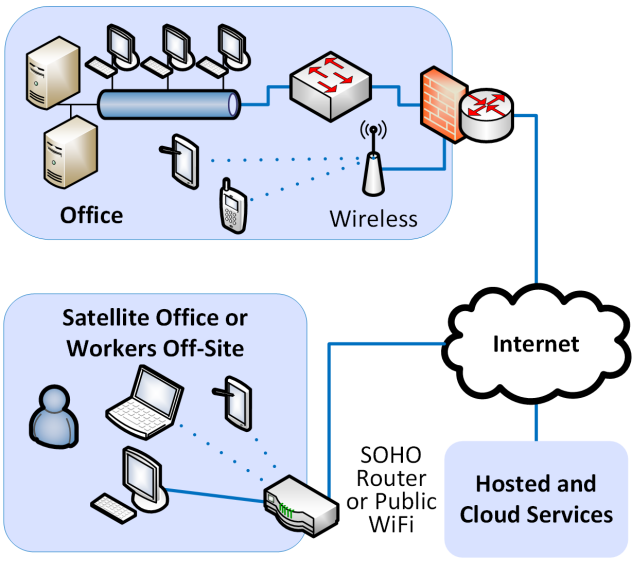


Figure 1 An example of a the infrastructure described for an SME for cyber security purposes

a healthy market of cheap, publicly available cyber security measures is available. The big issue is that beyond the endpoints SME IT infrastructures can vary enormously.

Network design engineers working with large organisations typically work from requirements documents, with some level of consultancy, to create their designs [18]. High level designs describe the infrastructure from endpoint to endpoint in the organisation by categorising the different types of site the customer has and aligning requirements to each site. If a technical cyber security requirement is noted in the requirements document then the equipment required to meet this requirement is included in the design.

A brief survey of network designs published by cyber security stakeholders, either to describe the way they have approached SME security initiatives, or products aimed at small companies, typically produces a diagram similar to Figure 1.

The derivation of the SME network diagram from a typical small site on a high level network design for a large organisation is obvious, however there are multiple indicators in this study's survey results that this is not an accurate representation of many SME infrastructures. It is however an infrastructure that the cyber security industry understands, and can already supply some suitable security measures for.

3.2.1 The Way the Survey Describes SME Infrastructures

The survey did not ask respondents to fully describe their IT systems, but there are multiple questions within the dataset which shed some light on their capability. Part of the issue is that it's impossible to define what a single 'normal' SME infrastructure model could look like, so the responses are considered given the size of the company. Combined with the open response questions and additional information participants asked to include in the dataset, a richer understanding of a variety of different infrastructures emerge.

Single Person Companies

The first thing to note with single person companies is that most do not have dedicated offices. The respondents working alone who did have their own office worked in industries where they might need a studio or workshop. 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. It is also thought that, for example, the furniture maker who responded to the survey would have chosen to have a dedicated workplace to reduce the quantity of sawdust entering their home, so the people with this size of company who do have dedicated offices are unlikely to be greatly altering their IT infrastructure.

All but one of these respondents have a company website, and all but one has a smartphone or tablet containing company data. All respondents have one computer containing company data, half have two. All of the respondents with company data in more than one computer have stated that they issue company computers or phones, so it can be assumed in many cases that the second computer is their personal machine. Half of the respondents with company data on only one machine do not issue company computers or phones, so it can be assumed that all the company data is on the respondent's personal computer.

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

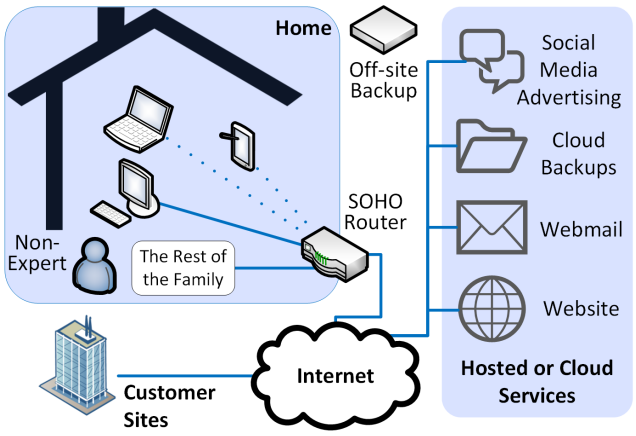


Figure 2 Infrastructure in single person companies

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

Five of these companies have their own social media accounts and use social media as their only or main source of advertising.

The resulting network diagram can be seen in Figure 2. The significant difference which can be seen between Figures 1 and 2 is the use of infrastructure more familiar in a home environment and the lack of any company owned network infrastructure.

Micro Companies

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

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

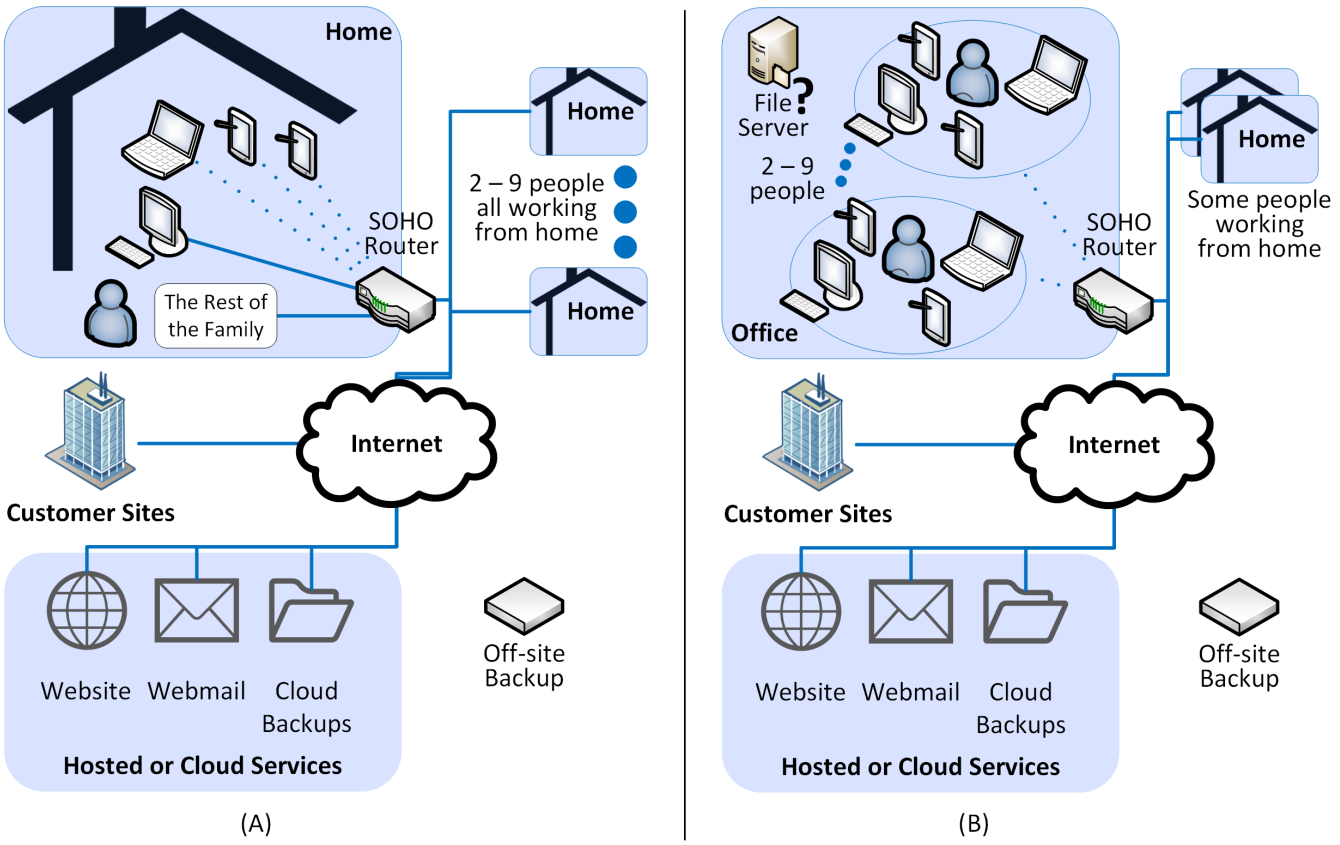


Figure 3 Infrastructure in micro companies: (A) Without an office; (B) With an office

due to a lack of a strict IT policy, rather than a higher requirement for multiple devices per person.

The increase in company size has not reduced the number of companies using webmail, and half the respondents still use cloud services, irrespective of whether or not they have dedicated offices. All these companies have off-site backups of their data. Three of the four without an office, and four of those with an office have suppliers or customers who provide a link into their IT systems, or who they allow to link into theirs.

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

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

The resulting network diagrams can be seen in Figure 3

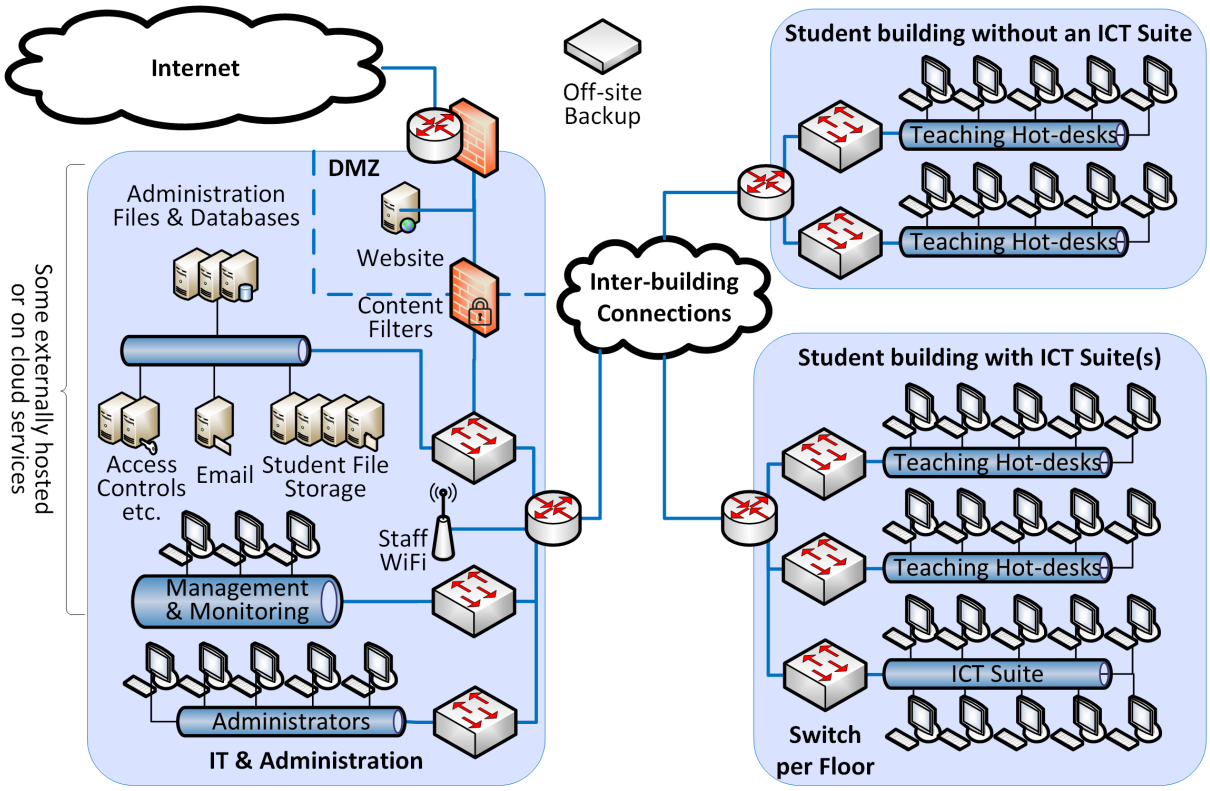
Small and Medium Companies

All of the respondents working in companies with between 10 and 249 people have dedicated offices. For the companies where all their staff are based in the same location their companies have become too large to use SOHO routers, meaning that they are beginning to use elements of corporate IT network infrastructure.

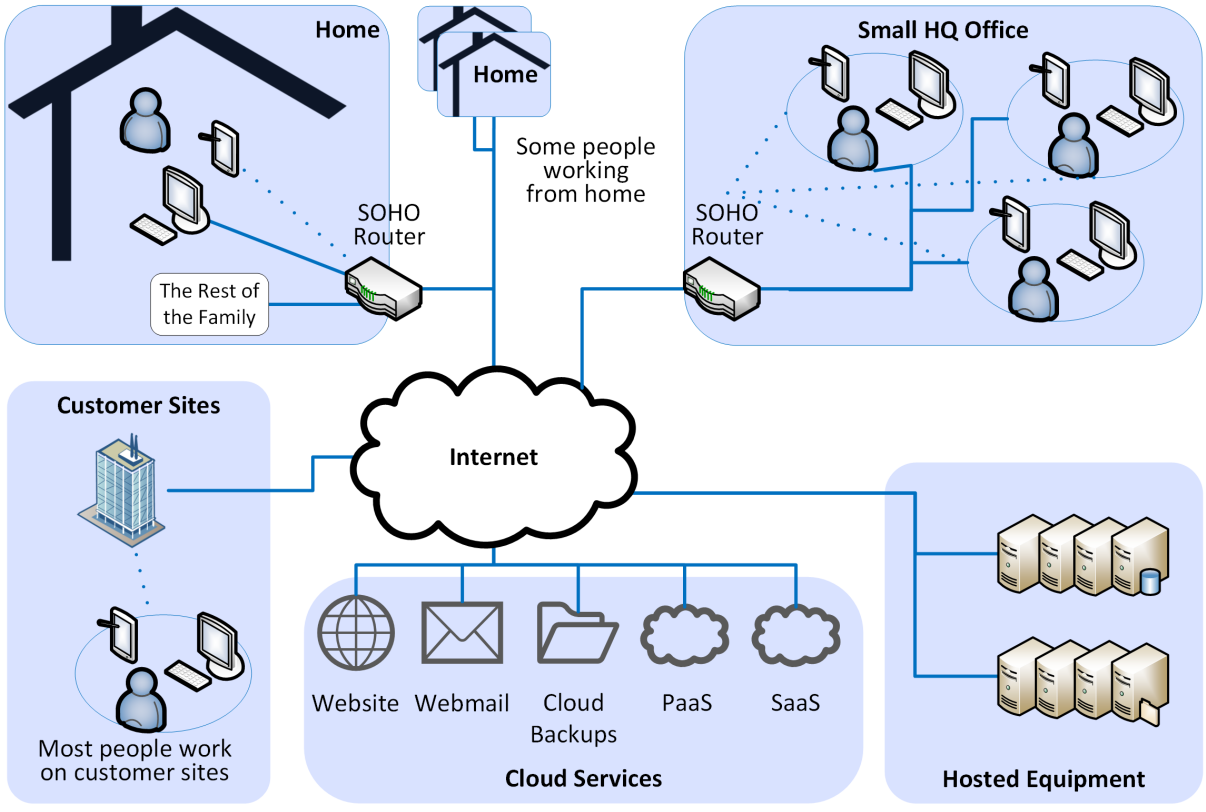
All the companies have websites, all have at least one computer and all but two have at least one smartphone or tablet each. All these companies are issuing IT equipment to some of their staff. Interestingly the number of phones and tablets per person in a small company emulates that of a micro company,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

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

All except two have dedicated IT support staff setting up computers, one of the two without dedicated staff is in the IT sector. All the companies let their operating systems auto-update, and have antivirus installed on



(A)



(B)

Figure 4 Infrastructure in medium-sized companies: (A) Respondent from the Education Sector; (B) Respondent from the Government & Defence Sector

their company issued machines. Six of the small companies and both the medium companies have suppliers or customers who provide a link into their IT systems, or who they allow to link into theirs.

All but two of these companies have their own social media accounts, but of those using social media only two agree that this is their only or main source of advertising, both in the IT and telecoms sector.

It can be assumed that the smallest of these companies have little difference in their infrastructure to one of the micro companies, as illustrated in Figure 3 (B). To show how infrastructures might evolve from this point, Figure 4 focuses on the two respondents from medium-sized companies, and their differences. Both of these companies have between 50 and 249 employees.

The first is in the education sector and, as discussed in Section 3.1, is felt to be the respondent 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 customers. The survey does not provide substantial information about the size or age of the student customer base, so as a guide information has been taken from one of the many schools and institutes who list their ICT facilities on their website. This is a school which has 162 staff, and 1420 pupils:

> *"There are 8 ICT suites spread across the school. These suites have 32 Windows 7 PCs and a Promethean interactive whiteboard... ...All teachers have access to a PC in their individual teaching rooms."[19]*

The second respondent from a medium-sized enterprise chose to describe their infrastructure in his own words:

> *"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 (for example the HR system) or as platform as a service (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."*

Neither of these companies are reflected in the SME network diagram described in Figure 1, which could be seen as being somewhere in between the infrastructures of two medium-sized SMEs responding to the survey.

3.3 How SMEs Experience Cyber Security

Q: What do you find most difficult about cyber security?

A: "Seeing the wood from the trees!"

3.3.1 Lack of Trust

Sections 3.1 and 3.2 highlight both the way the cyber security risks are presented to SMEs by other stakeholders, and the solutions the cyber security industry offer them. The lack of accessible evidence of a serious risk to respondents as small business owners, combined with a lack of cyber industry understanding of the way many small businesses operate, provides an explanation for some of the responses given to the survey.

Respondents were presented with an open response question at the end of the survey: *"What do you find most difficult about cyber security?"* Seventeen respondents chose to give an answer, many of the respondents talking about a lack of resource or knowledge, which will be discussed later in the section.

The following did not fit into those categories, and were coded as evidence of a lack of trust in sources of information or support in implementing cyber security:

> *"Knowing where to turn for up to date accurate unbiased information."*

> *"Lack of a single source of information. Inability to know the standard / quality of information we find on the internet. Scare stories"*

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

If SMEs are voicing their concerns over the biases of the cyber security industry in providing information, an obvious solution may be to direct them to one of the sources of information provided by government. For many of the respondents suggesting that their biggest concern is their own lack of knowledge, this may be the best answer. The post-Snowden reputation of the government has, however, not been left entirely unblemished in the eyes of one of the respondents. Only a broader survey would indicate if this response, to the question "Please list any requirements not mentioned in the last section that you need for good cyber security", is a widely held concern:

> *"Less ubiquitous, intrusive, poorly overseen, excessively shared government surveillance would be nice, as would a credible set of assurances that intercept data is not being passed among friendly governments and ultimately used to provide commercial advantage to competing companies. Also, it's important government organizations work to improve security rather than weaken it."*

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

The reality of the situation may be slightly different. Many of the respondents are suggesting that they are not sure where they stand where cyber security is concerned. The indication is that despite this all the respondents, even if they openly admit they do not care what cyber security is, are attempting to understand the risk they face, and as a result are implementing some form of cyber security measures in their companies. Other stakeholders may not become aware of this because SME owners are used to attempting any and all business functions themselves to keep their overheads to a minimum. Dictionary.com gives the definition of entrepreneur as follows:

> *"a person who organizes and manages any enterprise, especially a business, usually with considerable initiative and risk."* [20]

One SME highlighted this issue with the following comment, which can also been seen as one of the drivers for cyber security companies to focus their products elsewhere:

> *"Our infrastructure is very small and DIY, I don't think it would be worth your time."*

Another respondent admits that the results of this DIY approach are *"very hit and miss"* in terms of both IT and IT security.

The different attributes respondents are using to influence their self-defined security architectures are discussed in the following three subsections.

3.4 Cyber Awareness and Knowledge

With SME respondents looking to themselves to evaluate cyber risk and institute appropriate security measures it is understandable that five respondents mentioned an aspect of understanding risk management requirements and three named understanding cyber threats as the thing they found most difficult about cyber security.

There were four questions which were grouped during data analysis to establish when companies were potentially demonstrating a lack of cyber awareness — seeing passwords around the office, letting children install applications on a work phone, not having antivirus or doing updates, or not backing up files. None of the respondents reported all four of these occurrences, but seven indicated having experienced at least one.

That only 21% of respondents demonstrate a low awareness of one of the basic cyber security guidelines offered to non-experts is surprising given the concerns voiced in Section 3.1. Six respondents stated that a lack of time or financial resource is what they found most difficult about cyber security, surely because it makes instituting measures difficult, but in the context of maintaining or enforcing security having low resource could be seen as an advantage. Irrespective of the existence of formally recorded policies, the fact that the person evaluating the risk and instituting measures holds a variety of roles within the company allows them to continuously assess their risk. That a larger proportion of the company's employees come into daily contact with this person could also aid in enforcing good security practice. To establish the source of any cyber security knowledge demonstrated in the survey the respondents

were asked if they had read about cyber security online, or knew someone they trusted to advise them about security. 64% of respondents said they had done some self-led research, and 67% said they had a trusted cyber security adviser.

In order to measure the impact of these sources of knowledge on the respondents, their responses were compared with responses about confidence in ability to maintain security while working and how affordable they found cyber security.

The comparison shows that only those respondents who have done a significant amount of research, or are certain they have a trusted adviser, are certain they can afford cyber security measures. This group is populated by respondents in the IT industry, or those who hold an IT role. Those who have less knowledge, even when they have done a little research, are uncertain that cyber security is affordable.

Comparing knowledge against a respondent's confidence that they can work securely is more significant. Respondents who have sought no knowledge show a level of complacency, while the group with the most knowledge are less certain that they are capable of working securely. If the respondents with in-depth knowledge feel that cyber security is affordable but still lack confidence that they are able to maintain security this is a clear indicator that there are a lack of suitably adapted security measures for this sector.

3.4.1 Cyber Budgets

As mentioned in the previous section, lack of resource is clearly an issue for SMEs. In the survey respondents were asked how much they currently spend on cyber security and how much they could afford to spend to implement a security standard. Their responses can be seen in Figure 5. What is apparent is that the budget range a company is willing to spend on cyber security increases with the size of the company, as would be expected. Respondents capped their responses to the two budget questions below the highest value ranges offered by the questionnaire, so the maximum budgets are not limited by the responses it was possible to make.

Existing Cyber Security Budgets

The number of companies with a total cyber spend of less than £100 per year shows the level of constraint some companies are under, but also shows why the cyber security industry might find this sector less appealing when compared to the multi-million pound secure systems extremely large organisations deploy.

For some of the non-SME stakeholders discussed in this paper the logical solution may seem to be for the supply chain to begin forcing their suppliers to adhere to

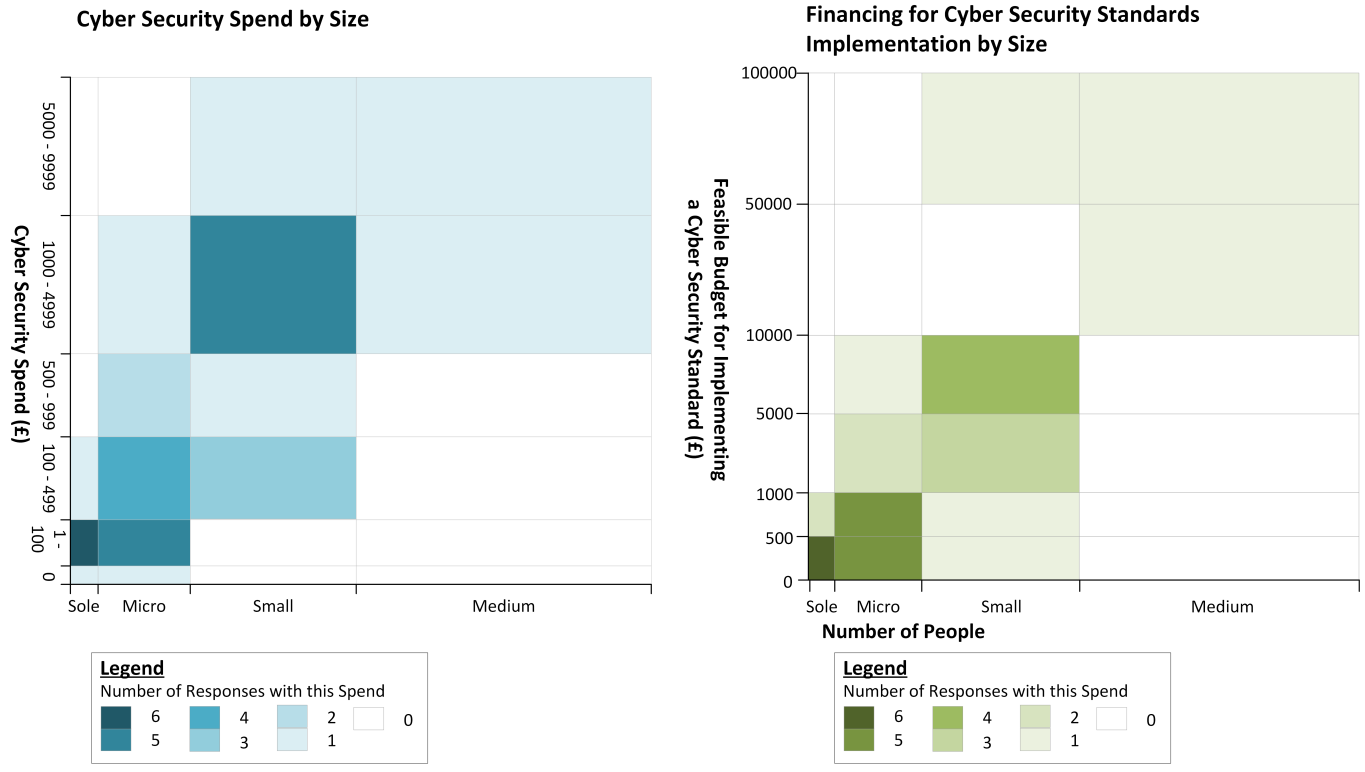


Figure 5 Cyber Security Budgets

Figure 6 Cyber Security Budgets Per Person

certain standards, motivating SMEs to provide adequate budgets and increasing security.

There is a fundamental flaw in this argument, which can be seen in Figure 6 where the budget ranges stated have been divided by the number of people in that sized company to provide a per person budget for cyber security.

The per person graphs show the heaviest population of responses as darker blocks. What can be seen in the graph covering the entire dataset is that the cost per person rises dramatically as company size increases, with no economy of scale until a company reaches a medium size.

The graph showing the budgets in the IT, telecoms, defence and security sectors, where the level of knowledge should result in a more risk-related solution, provides further insight into the barriers facing SMEs. In the small company group two clear bands can be seen, the first at £10-50 is matched in the micro companies, and is roughly the price of basic endpoint security. The second band, at £110-500, can therefore be assumed to show the cost of transitioning from home computer security, to what the cyber industry would recognise as corporate security.

The cost of entry for small SMEs to implement corporate style cyber security measures is extremely high. If a 'large' company of 250 employees had to implement cyber security at the price of £110-500 per person they would be paying £27,500-£125,000 per year. Survey respondents with medium-sized companies of up to 249 employees set their absolute maximum budget at £10,000. That top value was defined by a company in the defence industry, a sector known for extremely high cyber security risk [6].

What can be seen in the final two graphs are responses firstly for the professional services sector, followed by the 'other sectors' not in the IT, telecoms, defence, security or professional services sectors. There is a marked difference between the graphs – density of responses show that respondents in the professional services sector appear to be spending far more per person than those in any other sector, and there is not the transition to corporate security which can be seen in the IT etc. graph in either of these graphs.

The BIS Small Business Survey 2012 states that companies in the business services sector were more likely to make a profit than other sectors [21]. This leads to the consideration that the higher spend for professional

services is the combined result of having more scope in their budget, and a lack of the specialist knowledge that might allow the IT & telecoms sector to select suitable free tools.

The fact that the visible transition to corporate cyber security is not present outside of the IT & telecoms, defence and security sectors describes two separate business cases: the difference between financing cyber security as a business process and financing a saleable capability.

Affordability of Standards

Figure 5 shows that a large proportion of respondents from single person or micro companies stated that, even if cyber security standards became the expected norm in SMEs, they would only be able to implement one at a cost of less than £500.

An explanation of this may be found in the responses about annual turnover: 88% of sole traders and 23% of micro companies responding in this survey had an annual turnover of less than £79,000. These results are low – the BIS Small Business Survey 2012 states that the mean turnover for zero employee companies, was £127,100 and for Micro companies was £408,000 [21]. Zero employee companies are not the same as single person companies – they could have multiple directors, but 75% of respondents to the BIS survey have only one director. The BIS survey also shows that despite a higher turnover only 72% of companies this size made any profit in the year they took the survey.

In companies making only a modest profit cash flow is an important consideration for even small payments. While most SMEs expect to have to pay a certain amount for cyber security, and could potentially spend more than they currently do, these companies my be more open to accepting cyber security risk along with other high-risk decisions they have to make to protect their cash flow.

3.4.2 Cyber Risks, Requirements and the Art of the Possible

Risk

Risk has been mentioned on several occasions throughout this paper, and is seen as a central consideration in any decision about cyber security.

The responses to questions about the formal risk analysis process were as follows:

- 39% have done an in-depth risk analysis which included cyber security
- 48% keep the company's risk analysis, policies and backups up to date

These figures are low when compared to the BIS information breaches survey 2013, which shows 60% doing a risk analysis including information security. As discussed in Section 3.1, there were a far higher proportion of large and medium companies responding to the BIS survey than in the survey carried out for this study. A comparison would suggest that the likelihood of a cyber security risk analysis being carried out in a company is related to the size of that company.

Irrespective of whether a respondent had carried out a formal risk assessment the questionnaire asked respondents about the types of risks they faced.

- 82% have customer or supplier data to protect
- 61% have intellectual property (IP) to protect
- 58% have interconnected customer or supplier systems
- None have safety critical systems
- 42% have a website containing input fields
- 27% use predominantly social media advertising
- 94% know sales are dependent on company and employee reputation
- 6% risk losing customers if they do not implement a cyber security standard

As a whole the responses to the risk analysis section of the questionnaire demonstrate that SMEs are aware of reasons why they should be implementing cyber security measures. The barrier they face is one of a lack of knowledge, perfectly summed up by this respondent when asked what is most difficult about cyber security:

> *"Knowing about the risk management requirements to keep the threats under control."*

There is also the wider issue of SMEs managing to filter real information from what one respondent termed *"Scare Stories",* in order to provide a means to judge the impact and likelihood of a cyber attack. Without this information SMEs would find it difficult to judge

which risk management strategy is the most appropriate.

The only risk listed in the questionnaire where the financial impact can be easily quantified is the problem of data protection. The reason for this is the combination of the clearly defined financial penalties for failing to protect data, with the publication of several significant breaches and publicised (lack of) reaction from their customer base. In other scenarios it would be difficult for an SME to define a value range more accurate than "from half a man-power-day to re-install an operating system, to bankruptcy".

While the survey results suggest that SMEs are struggling to quantify their cyber security risk it does give some examples of treatment strategies they might be employing.

Taylor et al. define the four risk treatment options as avoid, reduce, transfer or accept [22].

There is some evidence in the survey of risk avoidance. One participant mentioned modifying their behaviour by *"not visiting dodgy websites"* as a means to reduce risk. This approach has the appeal of being a free cyber security measure, but it 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 have had to modify their behaviour in both their professional and private life, a sacrifice most employees would be unwilling to make for their employer.

The evidence of respondents employing basic cyber security measures, such as antivirus, probably indicates that companies are deploying basic measures for risk reduction. No explanatory relationship can be seen between a specific risk and the decision to employ these measures, so these measures are either fashionable or seen as due diligence irrespective of cyber security knowledge.

A high percentage of respondents stated data protection issues were a risk they faced, however, there was no explanatory relationship between this risk and the cyber security requirements respondents indicated later in the survey. This may well mean that, having carried out their basic risk reduction measures, the quantifiable risk provided by clearly outlined financial penalties is allowing SME owners to accept the risk.

The option often promoted by the cyber security industry as a catch-all solution for SMEs is the use of cloud services, which should allow SMEs to transfer cyber security risk. There are respondents using cloud services, but there is little evidence of respondents managing to successfully transfer risk. One issue may be in obtaining specific information from providers about how a cloud service treats customer data. However, a respondent highlighted a different issue in trying to integrate systems, with the following example:

> *"I believe it is the provision or lack of provision of features such as [allowing customers to integrate authentication systems] that have a significant impact on cyber security and the ability to implement it."*

The alternative? *"Each user has to remember yet another password."*

Another problem with advocating cloud services as a cyber security solution is the level of requirement a company has. If a company is having trouble securing their own data servers then purchasing Infrastructure as a Service (IaaS) may be the correct solution once their servers reach end of life. If, however, a company is so small that all data is stored on the staff's own computers, then purchasing IaaS is not an appropriate solution to their problem.

The final barrier to SMEs who might choose to use cloud services is actually imposed by cyber security risk. A respondent said the biggest difficulty they faced was that *"the laws governing [cyber security] is unclear many a times"*. This sentiment of not knowing where they stand legally, especially where acceptable handling of data is concerned, may result in a larger number of SMEs choosing to retain the risk within the company premises. The dataset also shows that, of the three small companies not using cloud services, one is a security company complying to ISO security standards, the second is the manufacturer who stated they felt pressure to adhere to standards.

The fact that cyber risk may be hampering the use of cloud services for SMEs has wider implications. For example, the impact of not being able to facilitate rapid expansion in startups can be the difference between an international public company and losing out to a competitor.

Requirements

As mentioned in the introduction the sample size precludes fully modelling specific requirements sets for different types of SMEs, however, there is sufficient

data to establish some influences to the way respondents are outlining their requirements.

The three concepts that regression analysis identified as significant in explaining requirements were:

- Basic knowledge (as defined in Section 3.4)
- Risk, predominantly of linking to another company's IT system, but also of losing IP
- The use of cloud services, including webmail and social media

The first thing to note is that these influencers provide evidence that respondents are highlighting requirements based on their business risk. This indicates that SMEs are evaluating their companies for risk, even where the respondent states that a formal risk analysis is not part of their business processes. Irrespective of their industry, the respondents are applying what knowledge they have of cyber security to independently resolve their issues.

The preponderance of requirements related to the interconnection of systems over other types of risk is felt to be related to a risk to reputation. Companies have been shown to survive large data breaches [23, 24], but allowing a company to link IT systems requires a higher level of trust. The loss of trust where a customer finds that an attack emanated from their supplier may cause that business relationship to break down.

The resources required for an attacker to target an organisation via the SMEs in its supply chain mean that these types of risks are likely to score very highly in a risk assessment, but comparably the SME's time and financial resources are extremely limited. This is not a trivial problem for SMEs to address.

IP also helped influence requirements, but to a lesser extent. In this case the risk is serious, but a company would have the right to keep a breach out of the public eye. There are also two other factors at play where IP is concerned. The first is that the protection of intellectual property is a well understood problem, with some legal paths for SMEs to use to protect their patents and copyrights. As the following respondent stated this recourse does not necessarily reduce cyber risk:

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

The second factor is one of resource. SMEs by definition have few resources, so when faced with a well-resourced opponent targeting them for their IP, the likelihood of an attack being successful would be increased. In this case they may feel that having a contingency budget for legal action once a copyright or patent is breached is the more financially viable option.

The Art of the Possible

Section 3.2 described SME infrastructures in the context of the suitability of existing cyber security offerings. What is also apparent from the infrastructure diagrams, is the lack of elements within these systems which are under the control of the risk owner. The most extreme case is the single person company, where the security of everything beyond the end point is in the hands of third parties, often holding no contractual requirement to provide good cyber security.

SMEs also have to develop their cyber footprint in order to advertise their companies. One observation from opening SME websites during the data collection process is that SME owners put a significant amount of information about themselves online, from the sole traders supplying home addresses, phone numbers and sometimes bank details on their websites, to those using their personal Facebook accounts to advertise their work. The result is that out of necessity to trade these individuals make themselves extremely easy to target.

This intersection of a large cyber footprint and a small IT infrastructure means that many of their highest impact cyber risks are in systems managed by organisations they interact with, for example:

> *"People are hacking accountant's login details to HMRC to submit false tax repayment returns"*

This accountant is right in identifying this business risk. If HMRC identifies irregularities in one account without identifying the associated cyber security incident, it could be the accountant's clients who get audited, and the accountant's reputation that is damaged. Seen in this context, the single risk reduction measure available – of employing a strong password – would not be overly reassuring.

This argument is emulated in Section 3.1 by stakeholders impacted by an SME's lack of cyber security, bringing the study full circle.

4 Conclusions & Future Work

What has been shown in this study is that the respondent group all employ some kind of cyber security measures, attempt to make judgements about requirements based on the risks that they understand, and all face significant barriers in terms of both resource and system ownership.

There is a lack of focus from the cyber security industry on the types of measures SMEs think they need within an SME budget – *"simple effective measures that are not to time consuming and require a great in depth knowledge of IT systems"*.

Section 3.1 also highlighted a lack of well evolved incentives encouraging SMEs to interact with cyber initiatives. This leaves SMEs attempting to handle to problem alone, while other stakeholders become increasingly concerned about the wider implications of their lack of cyber security.

Given the number of interacting and interlinked systems in the SME security ecosystem, the only solution to many of the problems faced would be for the dialogue between stakeholders to become more effective.

The results of this study can only be seen as preliminaries to a wider study – the dataset provides clues about issues in the SME cyber security dialogue, but the dataset is too small for these to be used in isolation.

As outlined in Section 2 it is difficult to engage with SMEs on this subject, mainly due to the lack of resource discussed frequently in the study. As such the opinions of the SMEs who have provided a response have been treated with significance despite their reduced numbers. The experiment was designed to be repeatable, so it may be that a broader sample of SMEs disprove some of the conclusions.

While the experiment could be repeated, the intention is to extend this research using unstructured interviews in a mixed methods approach. This allows participants to talk about the cyber security issues they find most important, rather than those other stakeholders in the ecosystem expect them to be concerned with.

In terms of resolving security issues in SMEs there are several potential strands of development:

- Respondents show a need for unbiased advice. SME owners are not the typical employee in need of awareness training, so further consultation on developing the content of SME-specific awareness programs is required. SMEs may, for example, require more information about vulnerabilities than tool implementation, to facilitate their capacity to self-assess risks.

- A means of providing accessible and accurate threat intelligence to SMEs, and potentially a selection of reviewed security tools suitable for their needs.

- There are two different cyber security business models accessed by SMEs. The corporate cyber security marketplace tends to be product-centric, providing a security layer for existing infrastructure. The home cyber security market is user-centric, configuration is simplified and cyber products are offered as part of larger purchases, or as software for evaluation. The respondents are indicating that there is a market for more cyber security in SMEs should some of the barriers they face be handled. An expansion of the user-centric business model beyond the endpoint may provide the best opportunity to bridge the gap between current home and corporate security offerings.

- The standardisation of a portion of the cyber measures employed in cloud computing services, and an improvement in the quality of information about the security offered as part of cloud service provision, so that there are less barriers for SMEs wanting to use these services.

Acknowledgements

With thanks to EPSRC for funding this project; Emma Philpott for acting as an SME sounding-board; Sadie Creese and David Upton for their invaluable advice and supervision; and Jassim Happa, Ioannis Agrafiotis and Jason Nurse for peer-reviewing the survey questions.

References

[1] European Commission. What is an SME? http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/sme-definition/index_en.htm.

[2] European Commission. EU recommendation 2003/361 concerning the definition of micro, small and medium-sized enterprises, May 2003.

[3] Department for Business Innovation and Skills. Business population estimates for the UK and regions 2013, October 2013.

[4] Mark Saunders. *Research methods for business students*. Pearson Education, Harlow, 6th ed. edition, 2012.

[5] Christina Goulding. *Grounded theory : a practical guide for management, business and market researchers*. Sage, London, 2002.

[6] ADS. Defence cyber protection partnership (DCPP), April 2014. https://www.adsgroup.org.uk/pages/65757387.asp.

[7] Information security breaches survey 2013: technical report - publications - GOV.UK.

[8] Warwick Ashford. Small firms lose up to 800m to cyber crime, says FSB. *ComputerWeekly.com*, May 2013.

[9] Information packages for small and medium sized enterprises (SMEs) - ENISA, 2006. www.enisa.europa.eu

[10] Tim Holman. ISSA 5173 the security standard for SMEs, March 2011. http://www.2-sec.com/2011/03/22/issa-5173-the-security-standard-for-smes/.

[11] Technology Strategy Board. Innovation vouchers for cyber security, July 2014. https://vouchers.innovateuk.org/cyber-security.

[12] HM Government. Cyber street, 2014. www.cyberstreetwise.com.

[13] Cyber essentials scheme: overview - publications - GOV.UK. https://www.gov.uk/government/publications/cyber-essentials-scheme-overview.

[14] ICAEW. 10 steps to cyber security for the smaller firm, November 2013.

[15] London Chamber of Commerce and Industry. Cyber secure: Making london business safe against online crime, September 2014.

[16] David Booth. The standard for information assurance for small and medium sized enterprises, March 2013.

[17] Robert B. Cialdini. Crafting normative messages to protect the environment. *Current Directions in Psychological Science*, 12(4):105–109, August 2003. http://cdp.sagepub.com/content/12/4/105.

[18] Priscilla Oppenheimer. *Top-down network design*. Cisco Press, Indianapolis, Ind, 3rd ed. edition, 2011.

[19] The mountbatten school website. http://www.mountbatten.hants.sch.uk/home/.

[20] Entrepreneur | define entrepreneur at dictionary.com. http://dictionary.reference.com/browse/entrepreneur

[21] Small business survey reports - GOV.UK. https://www.gov.uk/government/collections/small-business-survey-reports.

[22] Andy Taylor. *Information security management principles*. BCS, Swindon, second edition. edition, 2013.

[23] Target data theft hit 70 million. *BBC*, January 2014. http://www.bbc.co.uk/news/technology-25681013.

[24] Sony fined over PlayStation hack. *BBC*, January 2013. http://www.bbc.co.uk/news/technology-21160818.

Annexe A – Questionnaire Presented to SMEs

About Your Company

1. **What is your role within your company?**
2. **What industry sector is your company in?**
3. **Does your company have dedicated offices?** *(yes; no)*
4. **Which county is your company based in?** *(option list)*

The Size of Your Company

5. **How many people work at your company (including company directors etc.)?** *(just me; more than 1, less than 10; 10 or more, less than 50; 50 or more, less than 250; 250 or more)*
6. **What is your estimated annual turnover?** *(less than £79,000; £79,000 or more, less than £1.6million; £1.6million or more, less than £8.2million; £8.2milion or more, less than £41million; £41million or more)*

About Your Company's Technology Use & Budgets

7. **Average number of computers containing work files etc. per person?** (Excludes tablets & mobile phones. Includes looking at work emails on a home computer for example) *(0; 1; 2; 3 or more)*
8. **Average number of smartphones or tablets containing work files etc. per person?** (Including looking at work emails on a personal device for example) *(0; 1; 2; 3 or more)*
9. **How much do you currently spend per year on cyber security, including antivirus, firewalls, staff training etc. (£)?** *(Nothing; £100 or less; £100 to £499; £500 to £999; £1,000 to £4,999; £5,000 to £9,999; £10,000 to £49,000; £50,000 to £99,000; £100,000 or more)*
10. **If a significant number of SMEs were adopting a cyber security standard, allowing companies to become accredited for handling cyber security well, when would the set-up cost become unaffordable for your company?** *(£500 or less; £500 to £999; £1,000 to £4,999; £5,000 to £9,999; £10,000 to £49,000; £50,000 to £99,000; £100,000 to £999,999; £1million or more)*
11. **Does your company have a website?** *(yes; no)*

Your Cyber Security Knowledge and Awareness

12. **Please rate how these statements apply to you** *(Strongly Agree; Agree; Neither Agree or Disagree; Disagree; Strongly Disagree)*
    (a) I don't know what cyber security is
    (b) I don't care what cyber security is
    (c) Someone has made me think cyber security might be important
    (d) The press have made me worried about cyber security
    (e) I have done some reading about cyber security online
    (f) I feel confident that I can maintain a suitable level of cyber security whilst I work
    (g) I have someone I trust who can provide information about cyber security when needed
    (h) I have thought about cyber security and decided it's out of my budget

Mini Risk Assessment

13. **Please rate how these statements apply to your company** *(Strongly Agree; Agree; Neither Agree or Disagree; Disagree; Strongly Disagree)*
    (a) We have customer or supplier data that we need to protect
    (b) We have intellectual property that we need to protect
    (c) We have suppliers or customers who provide a link into their IT systems, or who we allow to link into ours
    (d) We have lost / may lose customers because they are beginning to request that we are that we are certified with security standards (i.e. ISO 27001, PCI-DSS, IASME)
    (e) Company sales are heavily dependent on the company and its employees maintaining a good reputation
    (f) We have a website which allows people to login or input information into forms
    (g) Using social media or recommendation websites is our main source of advertising (Linkedin, Twitter, RatedPeople.com etc.)
    (h) We have safety critical systems (impacting on health and safety) accessed or controlled by our computers/mobile phones
14. **Please list any specific reasons that you think your company will come under attack**

Behaviour and Current Cyber Security Measures

15. **Are these statements true or false in your company?** *(true; false; don't know)*
    (a) People at my company use Facebook, LinkedIn, and Twitter etc. for advertising, job applications or organising social events.
    (b) Some or all people at my company have a computer or smart phone issued to them
    (c) People have the ability to install anything they wish on their work computers irrespective of company policy
    (d) Anyone at work can access any file on company shared file servers
    (e) People use webmail accounts (Gmail, Hotmail etc.) for work
    (f) I have seen people's passwords for work systems written down around the office

(g) I let my children play with my my work phone or tablet and choose what apps to install

(h) The company favours use of free or open source software

(i) The company has its own social media account

(j) The company have dedicated IT support staff to set up our computers

(k) People use their own or customer USB sticks to exchange files at work

(l) The company uses cloud services to store data or use applications (including Dropbox etc.)

(m) Our computers have antivirus software and allow Windows (or equivalent) to auto-update

(n) All our files are backed up and stored somewhere else in case there's a fire

(o) The company has done an in-depth risk analysis which included cyber security

(p) The companys risk analysis, policies and backups are kept up to date

(q) The company is ISO 27001 certified

(r) All the doors and windows are locked when the office is empty

Your Cyber Security Requirements

16. **Please mark how important each cyber security issue is to you.** Please include those already implemented and any which are on your cyber security wish list. *(critical; important; optional; not useful; I don't know what this is)*

    (a) Basic Knowledge and Good Practice

    (b) Disaster Recovery & Backups

    (c) Resilience

    (d) Cyber Security Standards

    (e) Compliance for Insurance

    (f) Physical Security of Equipment

    (g) Reputation & Social Media

    (h) End Point (Computer/Server) Security

    (i) Smartphone or Tablet Security

    (j) Network Security

    (k) Website Security

    (l) Security in the Cloud

    (m) Cyber Incident Management

17. **Please mark the types of requirement you have for the issues you highlighted in the last question. You can select as many options as you like. Please include those already in place and any which are on your cyber security wish list.**

This section was filtered to show only items that respondents marked as critical, important or optional in question 16. For each issue they highlighted they could choose from the following six requirement types: advice guides; awareness training; consultancy; dedicated staff; implemented policy and implemented technology.

18. **Please list any requirements not mentioned in the last section that you need for good cyber security.**

19. **What do you find most difficult about Cyber Security?**