Knowledge Transfer Network

ICT

LANCASTER UNIVERSITY

# Small Business: Cyber Security Survey 2012

## Security Lancaster

# Foreword

## Contents

**Mr Tony Dyhouse**
Director Cyber Security

**ICT Knowledge Transfer Network**

Despite major advances in technology, communication often remains a human weakness. The SME sector has difficulty in engaging with large corporates and industry, yet these customers may represent their route to business success. Government needs to demonstrate impartiality and fairness, so is reluctant to engage on an individual basis, and all sectors struggle with the different ethos and culture of our academic institutions and the experts within. The ICT KTN strives to break down these barriers to communication, and act as an enabling hub for these parties in order to encourage innovation, knowledge transfer and success. This intent is fully achieved by our programme of work with Lancaster University and InfoLab21.

The success of CSC2011 served as a catalyst for CSC2012, and the realisation that such a gathering of attending sectors could serve to provide useful statistics and insight. I am pleased to be involved with the production of this report and ICT KTN is planning to extend their partnership with Lancaster University going forward. I hope our work and future reports will inform and assist all sectors to work collaboratively to ensure efficiency and success.

**About the ICT KTN Co. Ltd**

The Information and Communications Technology Knowledge Transfer Network (ICT KTN) is an industry-led initiative funded by the Technology Strategy Board and focused on ICT Knowledge Transfer as a stimulus to economic growth. The ICT KTN seeks to deliver improved industrial performance through innovation and collaboration, and provides an independent business voice to inform Government of the needs of the sector.

https://connect.innovateuk.org/web/ictktn

## Executive Summary

Most people would agree that both the rate of adoption of digital technologies and the pace of change within the digital industries are ever increasing.   Consumers and businesses alike are presented with an ever changing landscape where technologies are becoming more powerful, perhaps more complex and certainly more available. Customers want higher levels of service and their product 'now' whilst staff want to be able to balance work and life better with the adoption of agile or virtualised working practices.  Digitally based solutions can offer the means for small business owners to achieve this.  They are able to communicate more easily with clients and suppliers, transact business quicker, give great visibility to partners and stakeholders alike and offer staff more flexible working conditions.  Ultimately, in order to compete, companies are almost expected to embrace digital systems.

This report seeks to ask the question: "in this headlong rush to embrace digital systems and practices, what security measures are being (or could be) put in place by smaller companies to protect their businesses, their staff, their clients and wider stakeholders."   The Authors feel this question is important as, whilst the benefits of utilising digital systems are widely documented, the exposure and risk to those smaller businesses adopting them is less well known with the consequences and pitfalls of experiencing IT security issues being potentially catastrophic.  With the vast majority of the economy being made up of and driven by small businesses the risk and likelihood of serious IT Security issues can only increase as more take up digital systems and practices.  A better understanding of how IT Security in small business is addressed now will help inform more secure business practices going forward, ensuring that businesses are able to embrace technology and prosper without exposing themselves to unwanted business risks.

### Background

The information in this report was gathered during the registration process for a joint Security Lancaster/ICT KTN event held on September 3rd 2012.  That events aim was to gather a range of consumers and suppliers of digital technologies, along with Lancaster University Academics, to discuss aspects of how IT Security is addressed in small business.   There were 118 registrations for the event with 98 attending on the day.  All 98 attendees completed an initial business questionnaire (phase 1) with a subset of 48 of those companies completing an IT specific survey (phase 2). This activity was intended to be an initial exercise to identify areas of interest/concern as well as highlight specific areas for further, more in depth, research activity.

### Findings

Whilst it is recognised that the scale of the survey may not provide a robust or statistically significant output in terms of data that can be mapped across the small business population as a whole the initial findings were of interest and gave useful insight in to further areas to be explored in a more extensive exercise.

The key findings were as follows:

- 98% of respondents cite IT/Cyber security as a high business priority for them but only 43% actually those businesses have an actual IT security policy in place.
- 45% of respondents have ongoing IT security training for their staff whilst 20% provide this education only during induction then leaving the employee to educate themselves.
- Only 59% of all respondents outsourcing services have any form of IT policy protection.
- 55% of respondents were unaware of IT compliance requests from their clients and 66% unaware of requests from their suppliers or partners.
- The top four drivers for IT expenditure in the respondents are; protecting customer data (34%), complying with laws and regulations (15%), business continuity (11%) and preventing system downtime and outages (11%).
- Prioritisation of IT expenditure does not translate to spend on security with nearly half (47%) of respondents spending less than 5% of their IT budget on security.
- Respondents were optimistic regarding any rising threat of future security incidents in the next year with 62% believing they would be roughly the same as previously experienced and 85% expecting incident numbers to be the same or better.
- Respondents generally saw incidents as minor (~50% accidental and 50% malicious) with only 10% believing they had suffered a serious malicious directed incident

Respondents were best able to identify incidents of ‘Infection by malicious software’ and appear much more able to define the severity of such attacks. Conversely 20% of respondents are unsure whether they had been attacked by a malicious external party

## Conclusions

This initial survey would appear to show that respondents do recognise the importance of IT Security, particularly with respect to protecting their customer’s information and complying with legislation. There also appears a reasonable level of awareness of types of minor IT security incident types. What does become apparent though is an issue in translating threat awareness directly to business practice. There is a low commitment to significant spend on IT Security at a budget level or on-going awareness training for staff and little scrutiny is given to provision around external outsourcing. In addition there is also a clear issue for businesses in attaching value to or predicting the cost of IT Security incidents. This translates to a real issue in mapping any cost/benefit around adopting a greater level of IT Security in small businesses.

## Recommendations

There are definitely areas of this research that need to be explored in more depth but one key recommendations the Authors would suggest is this work be expanded in partnership with business to create a toolset to enable small businesses to develop clearer impression of their bespoke costs/benefit profile relating to IT/Cyber Security.

# Introduction

The Small Business Cyber Security Survey was conceived as a response to a range of business questions that Lancaster University were being asked regarding the topic of cyber security. For a number of years Lancaster University has been running an annual conference focusing on business issues around cyber security culminating in the Cyber Security Conference series (Security Lancaster, 2012). For the past two years these conferences have been run in partnership with the Cyber Security working group of the Information Communication Technology Knowledge Transfer Network (ICT KTN). The conferences have focused on providing a valuable business to business space focused on cyber security where companies in the region, and nationally, can come together to network, share best practice and understand the issues other companies may be facing.

For this reason, the organisers of the conference decided to formalise this information gathering exercise in the hope of providing a valuable resource for businesses in understanding the types of cyber security concerns and issues that the region as a whole is facing. The Authors intend to provide a longitudinal study, which will run alongside the Cyber Security Conference series, which will provide the foundation to understand the evolution of regional business cyber security concerns.

This is the first report in a planned series and so represents the Authors first attempt at designing a survey methodology that truly captures regional cyber security business concerns. This methodology is identified in the next section and the feedback and understanding from running such a large scale business survey will enable us to improve our methodology in subsequent survey iterations. Where the Authors felt there were issues with the data or methodology these have been highlighted.

Throughout this survey the reader will note that the Authors have chosen to follow the Office of National Statistics in treating the term Data as plural. The data has also been made available online as an open resource for verification and further use by other interested parties.

# Survey Methodology

The survey was completed in two phases and focused on the registrants for the annual Cyber Security Conference (CSC2012) held at Lancaster University in conjunction with the ICT KTN[1]. It is worth noting that the group of people that provided survey responses were self-selecting with an interest in cyber security. This produces a natural response bias as the responders hold issues surrounding cyber security in high regard.

## Phase One: Business Population

The first phase of the survey was conducted as part of the conference registration. Registrants were asked questions on the size and type of business, and several questions regarding their business needs and barriers to growth.

The questions regarding the nature of the registrants business sought to identify the demographic of those with an interest in cyber security in the region. These questions were structured using the classification used by the Department of Business Innovation and Skills (BIS) when completing the

[1] Information on CSC2012 can be found at http://www.security-centre.lancs.ac.uk/conferences/csc2012/

business population estimates in order to draw regional and national demographic comparisons and to understand any demographic bias.

The Authors further sought to understand the registrants' opinion on business aspirations, growth barriers and required assistance. A series of free text questions were asked to elicit this information with the responses subjectively classified and grouped dependent on answer sentiment as interpreted by the Authors. Readers should be mindful of this when trying to further understand or extrapolate data associated with these responses. The registrants were also asked whether they currently produce a cyber security product in order to comprehend the demographic in light of their responses in the second phase.

Multiple people from the same company were permitted to register for the conference and were required to submit answers to Phase One. In the case where multiple answers from the same company were obtained the registrants job role was the deciding factor as to which answer to utilise in the analysis. More senior roles were selected in favour over junior roles, based on the assumption that the senior role would have a clearer idea of company direction and growth potential. This yielded 73 usable results for analysis of Phase One data.

### Phase Two: Technology use and Cyber Security Incidents

Phase Two was identified to the registrants as an optional online survey motivated via the availability of a prize. Responses to Phase Two could be tracked back to Phase One via a unique identifier in order to link business population information with the types of issues companies face. All of the responses given in Phase Two were objective in nature.

The questions asked were in line with those reported as part of the Internet Security Breach Survey (PWC, 2010) (PWC, 2012) which is conducted every two years by PWC and published at the InfoSecurity Europe conference. By posing comparable questions the authors were able to evaluate the survey responses against national statistics for a range of company sizes. Where possible when comparing this survey to the ISBS 2010 and 2012 reports the comparisons are drawn directly to the data regarding small businesses. Where specific data for this sector is not available then the aggregate figures are used from the survey.

At several points in this Phase, questions are asked with responses of the type "none of the above", "other" and "unsure" available. This introduces a methodological issue which potentially leaves a wide scope of interpretation for the respondent. For example does "none of the above" mean that none of the other listings apply and the respondent has experienced and event or the respondent has not encountered the event under investigation at all? For this reason, the reader is advised to use caution in extrapolating meaning from these data. These catch all, default options will be removed in further surveys in order to provide a more detailed analysis.

Utilising the data from Phase One and combining it with the returns from Phase Two provided 47 usable responses. The Authors would like to highlight to the reader that at this point there is a step change in the sample size from 73 to 47. The reader should therefore adjust their consideration on the reliability of the data, given the reduced sample size

# Phase One: Business Population

During the analysis of the Business Population that registered for the Cyber Security Conference 2012, the Authors used the standard EC SME (Micro, Small and Medium sized businesses) Definition (European Commision, 2005). The main factors which determine the size of the company are:

- **number of employees** and
- either **turnover** or **balance sheet total**.

| **Company category** | **Employees** | **Turnover** | or | **Balance sheet total** |
|---|---|---|---|---|
| Medium-sized | < 250 | ≤ € 50 m | | ≤ € 43 m |
| Small | < 50 | ≤ € 10 m | | ≤ € 10 m |
| Micro | < 10 | ≤ € 2 m | | ≤ € 2 m |

Table 1 EU Classification System For Small to Medium Enterprises

When applying these limits, as shown in Table 1, to the collected data represented in Figure 2 and Figure 1 we can see that 55% of the registrants would be classed as Micro businesses, 29% as Small business and 12% as Medium businesses.

Further differentiation cannot be drawn based on the turnover figure as anything above £500K was grouped together. This level of detail will be asked during the next survey in able to draw direct comparisons but also aid a more sophisticated analysis of the registrant business population.

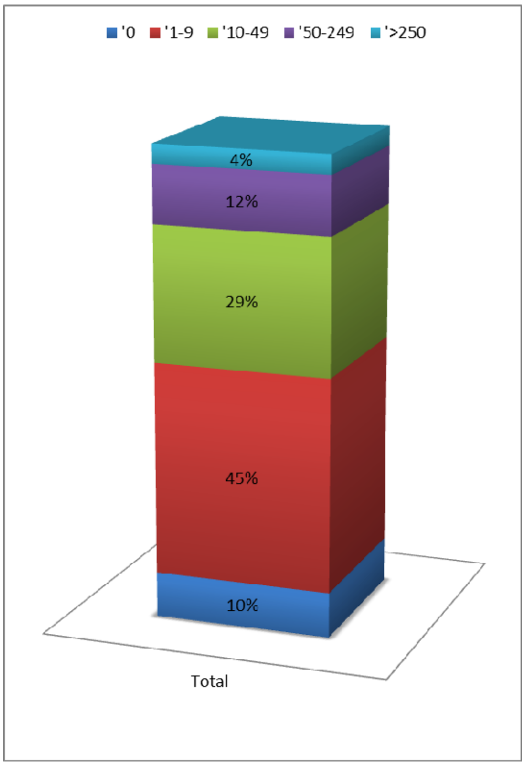

Figure 2 Business Size of Respondents by Head Count

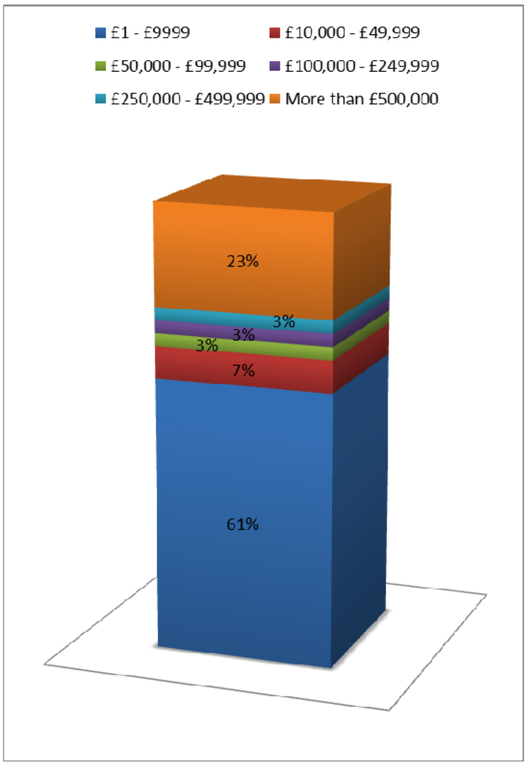

Figure 1 Business Size of Respondents by Turnover

By way of further analysis, Figure 3 shows a topology map of the number of companies plotted against head count and turnover. This view of the data clearly shows a “no-man’s land” in business size between high turnover and low turnover of the registrants where companies are polarized into either Micro or Small in terms of head count, but the fine grained analysis of the turnover also groups companies at the very small end or at the larger end. The reason for this is not clear, however, three possibilities are postulated by the Authors:

1. There this is a problem with the survey approach producing a bias in the these data
2. There is a reticence of the respondent to provide accurate turnover data
3. The audience target for communication regarding this event naturally has this profile

The data do not provide a clear indication as to which possibility should be considered correct in this instance. Therefore, future work must attempt to further understanding as to whether this demographic is representative of the wider business community in the region and if not by how much. The survey could be extended to provide further stratification of the turnover in order to enhance the understanding, particularly given the micro business nature of the registrants in this phase.

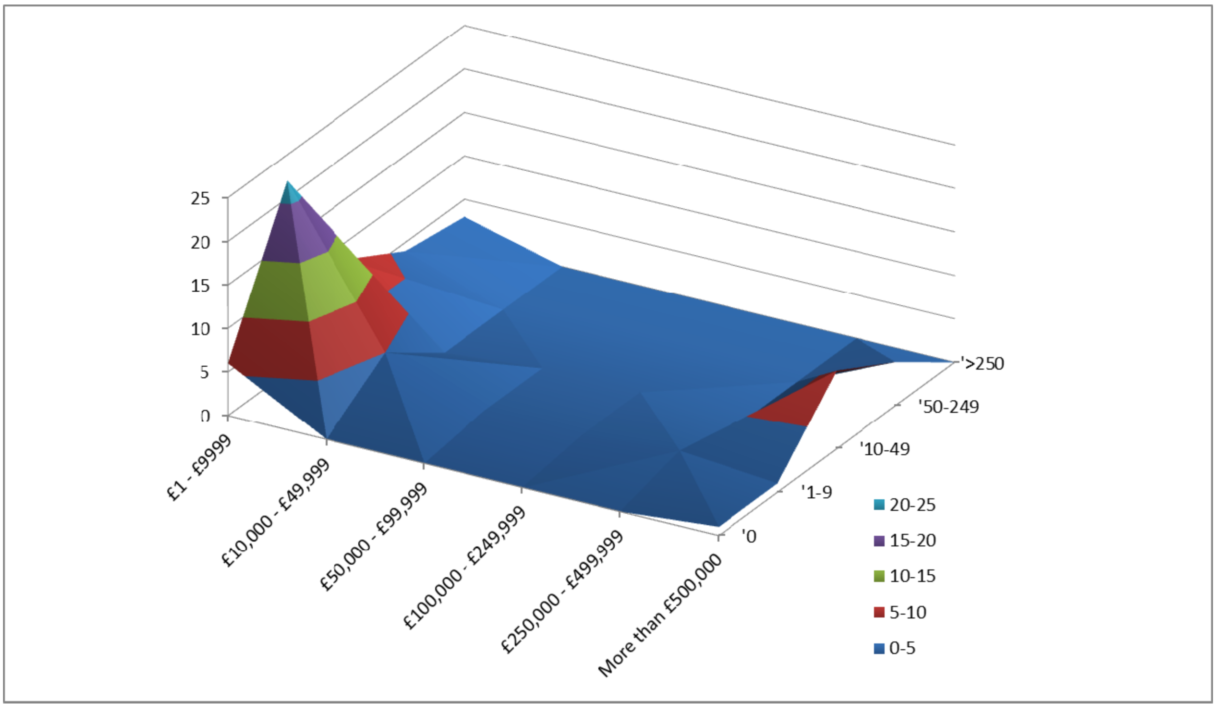

**Figure 3 Demographic Topology of Registrants by Head Count and Turnover**

## Security Product Provision

During Phase One the registrants were also asked if their company produced a product or service which they considered to be an offering in the cyber security domain. It is interesting to note that the data in Figure 4 indicates that there are companies that are non-ICT based who believe they produce a cyber security product. Since the completion of the Phase One, the Authors have developed a more sophisticated understanding of the cyber security product and service marketplace.

This enables the classification of the offering as either of the following:

- **Primary Producer:** A cyber security product or service is produced by a cyber security company
- **Differentiating Producer:** A non-Cyber Security company who differentiates it core business offering from its competitors using Cyber Security
- **Diversifying Producer:** A company whose core business lies outside Cyber Security, but has chosen to start a new product line or service provision in cyber security.
- **Consumer:** A company only consumes cyber security products in order to provide its core business offering

Clearly such levels of analysis are not available from a simple yes or no answer, however, it is reasonable to assume that those registrants that responded ‘no’ would be consumers, while those who responded ‘yes’ and are classified as Information and Communication are Primary Producers. The remaining categories of differentiating and diversifying producers cannot be distinguished but broadly the remaining companies that fall outside the two classifications could be considered in this group. This gives rise to the data contained in Table 2.

| | **% of Registrants** |
|---|---|
| **Primary Producer** | 27% |
| **Differentiating or Diversifying Producer** | 18% |
| **Consumer** | 56% |

**Table 2 Registrant Classification of Security Product Type**

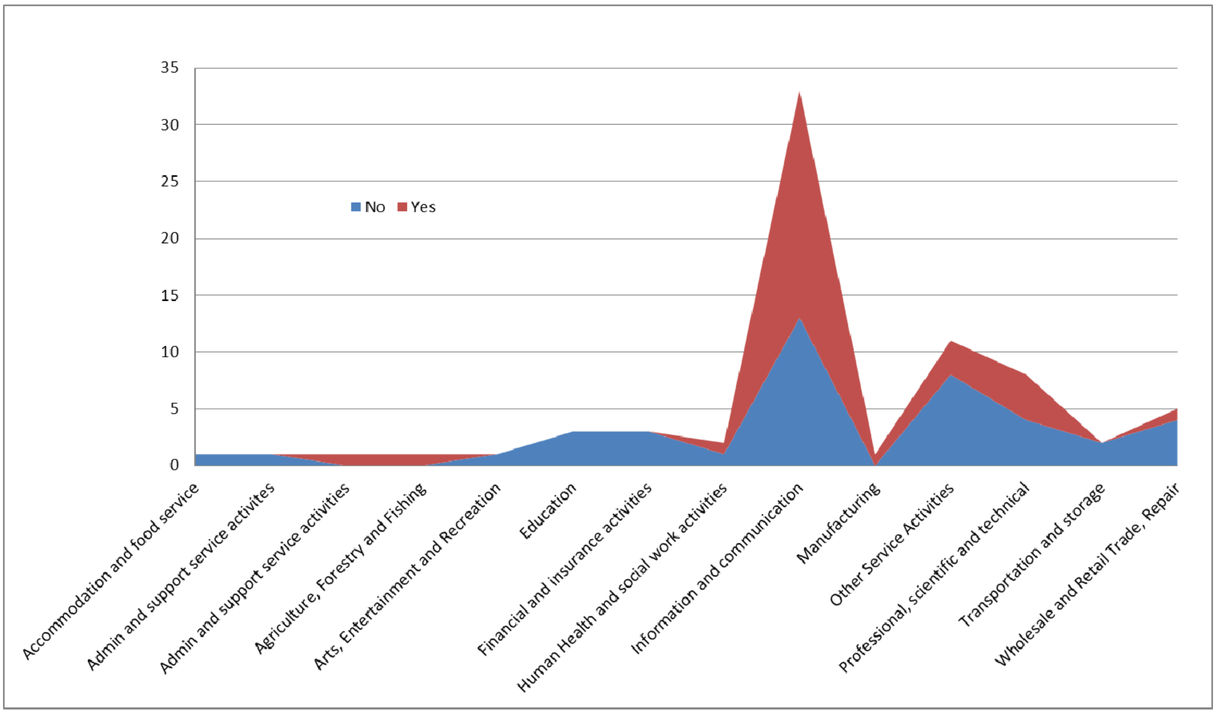

**Figure 4 Registrant Response to Whether They Produce a Cyber Security Product**

In future surveys the security product question will be extended in order to determine the type of cyber security producer. This measure will also provide a baseline for the conference organisers in order to measure their success at being able to diversify the attendees of the conference.

## Comparison to the UK

Registrants were asked to identify the business sector they belonged to using the classifications used in the BIS Business Population Estimates Report (Department for Business Innovation and Skills, 2011) Figure 5 shows the comparison between the registrant data (in Red) and the UK wide data presented in the 2011 report (in Blue). It should be noted that the data from the BIS report includes businesses of all sizes while the data obtained for this report focuses mainly on small and micro businesses as identified previously. Also note that the population estimates also include more classifications however, those that have been given a 0% from the registrant data are not given here.

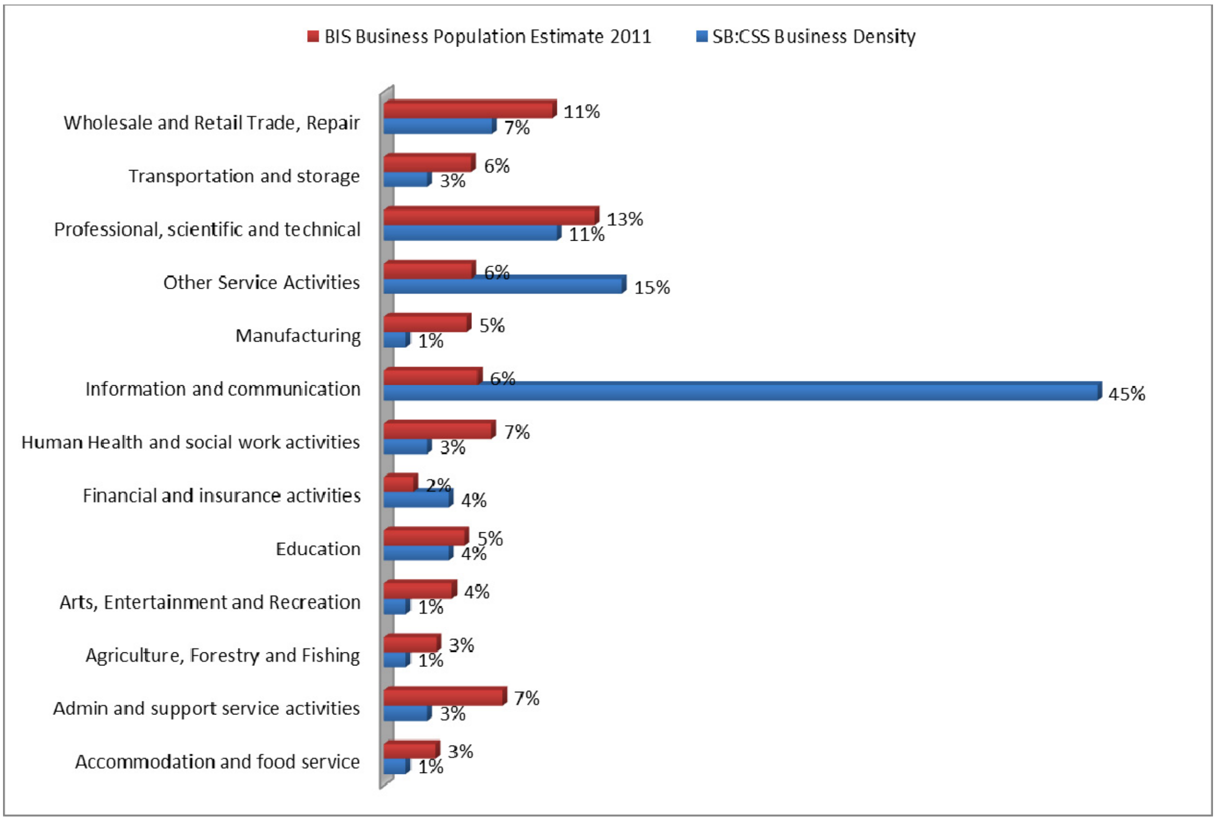

**Figure 5 Business Density Comparison of Registrants to UK Business Population Estimates**

It can be seen that profile of the registrants corresponds to that of the national level profile. However, two sectors significantly buck the national profile; Information and Communication and Other Service activities. The significant representation of Information and Communication companies represents the natural bias of companies that would naturally self-align with cyber security. It also demonstrates the bias in the utilised communications channels in order to recruit people to the event and the lead partner in the event, the ICT KTN. Largely ICT related networks were utilised to spread information regarding the event and so this peak represents the nature of those companies affiliated with those networks. The spike in other service activities may be due to a problem with the design of the registration questionnaire. It may not have been clear to registrants what was meant by each category and no additional explanation beyond the label was given. Therefore, without further clarification registrants chose to select a “catch all” response to describe their core business activities. In future surveys, endeavours shall be made to provide further details on what is meant by each classification label in order to help with the sector selection.

It is difficult to draw direct comparisons to the sectors surveyed during the ISBS2012 report due to the different classification systems. However, the Authors have provided an attempt at a conversion matrix as given in Table 3. It should be noted that the separate classifications of Technology and Telecommunications from ISBS2012 have been combined into a single group and are compared with "Information and Communication", and "Professional, Scientific and Technical" from SBCSS in order to make translation easy. A graphical comparison of the data can be seen in Figure 6.

| Survey Classifications | | Results | |
|---|---|---|---|
| **SB-CSS:2012** | **ISBS:2012** | **SB-CSS:2012** | **ISBS:2012** |
| Financial and Insurance Activities | Financial | 4% | 17% |
| Information and Communication | Technology and Telecommunications | 56% | 27% |
| Professional, Scientific and Technical | | | |
| Accommodation and Food Service | Travel, Leisure and Entertainment | 3% | 2% |
| Arts, Entertainment and Recreation | | | |
| N/A | Utilities, Energy and Mining | 0% | 2% |
| Manufacturing | Manufacturing | 1% | 6% |
| Transportation and Storage | Retail and Distribution | 10% | 3% |
| Wholesale and Retail Trade, Repair | | | |
| N/A | Property and Construction | 0% | 2% |
| Education | Government, Health and Education | 7% | 21% |
| Human Health and Social Work Activities | | | |
| Admin and Support Service Activities | Other | 19% | 20% |
| Agriculture, Forestry and Fishing | | | |
| Other Service Activities | | | |

**Table 3 ISBS2012 to SB-CSS2012 Business Classification Matrix**

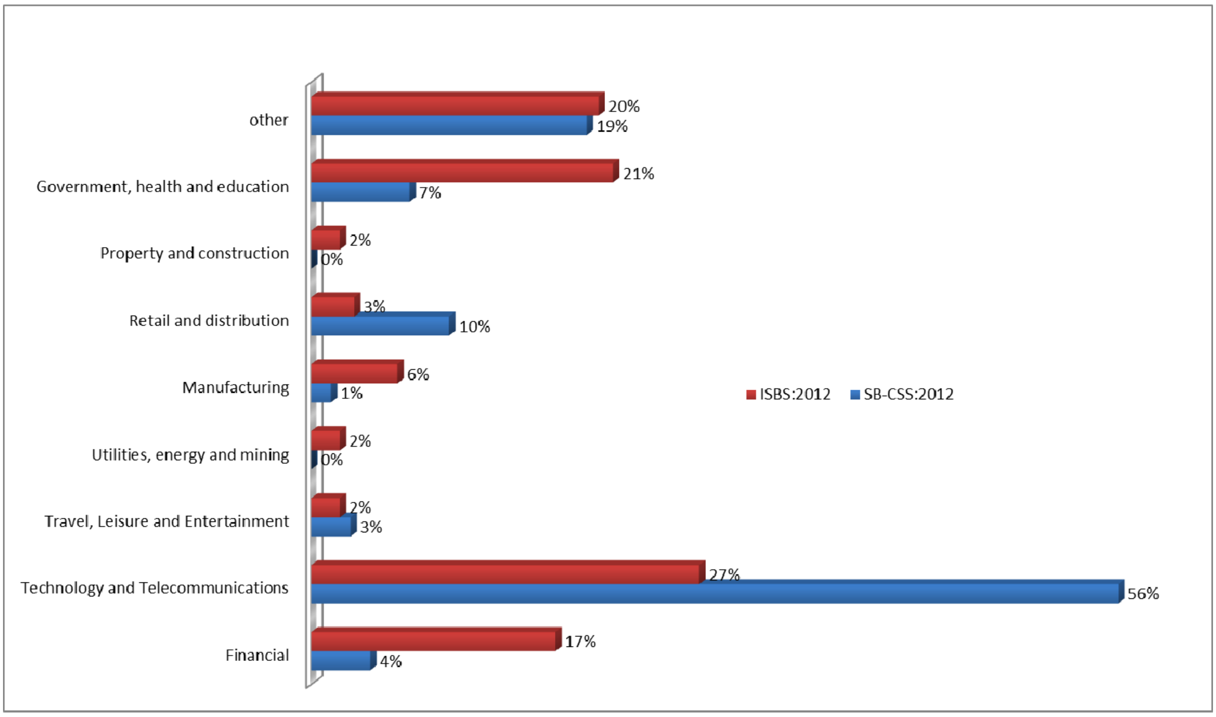

**Figure 6 Comparison of ISBS:2012 to SB-CSS:2012 Business Types**

It can be seen from the data that there is a clear disparity in some key areas. Most notably with the dominance of responses from ICT companies. The explanation of this dominance from the comparison with the BIS business population data holds here as well. It is clear that the nature of the targeted communications regarding the event naturally biased the delegates and hence respondent data. Generally the two data sets here are divergent and should therefore be taken into consideration in the comparison to Phase Two results and there is a clear need to engage a wider business community in order to gain a broader set of results.

## Aspirations, Growth Inhibitors and Assistance Required

This section is comprised of a subjective classification of the sentiment of the responses given to these questions by the registrants to the conference. Each free text answer was classified based on the sentiment and the Authors feel that as an exploratory exercise in understanding the aspirations, growth inhibitors and required assistance, of regional businesses success has been achieved.

Due to the nature of the business demographic as shown in Figure 2 the majority of the businesses have less than ten employees. This fact, coupled with the nature of the answers which have been classified as “Nothing” or “None” in the following data references the start up nature of the businesses themselves. i.e. the businesses are primarily focused on survival or completing their initial business plan and have not reached the stage of considering the next stage. They are also achieving all of their aims as a start up company. There appears to be a correlation between those responses that are categorised as Nothing or None for the Authors to make the inference that the registrants who responded in this fashion are all similar.

### Aspirations

**What have you always wanted your organisation to do but have not been able to get started?**

The purpose of this question was to identify the aspirational aims for their business in order to understand what the companies attending the cyber security conference want to do but felt restricted in doing. The resultant data is given in Figure 7.

The data show that the key pressure point for the majority of companies is general ‘business development’ advice which is congruent with the Micro and small nature of the businesses represented. Naturally given the company demographic that registered for the conference it is not surprising that next biggest aspirational area is ‘software development’. However, the results for ‘improve security’ and ‘security as a business’, holds with the Authors more sophisticated understanding of the cyber security market place as these areas can be interpreted as ‘Differentiating Producer’ and ‘Diversifying Producer’ respectively.

There are various activities being led regionally that would enable businesses to access software development support. However, this data demonstrates that the businesses need either be made aware of, or have provision made available to them, in order to access ‘Business development’ advice and advice regarding how businesses could be developed in the cyber security industry.

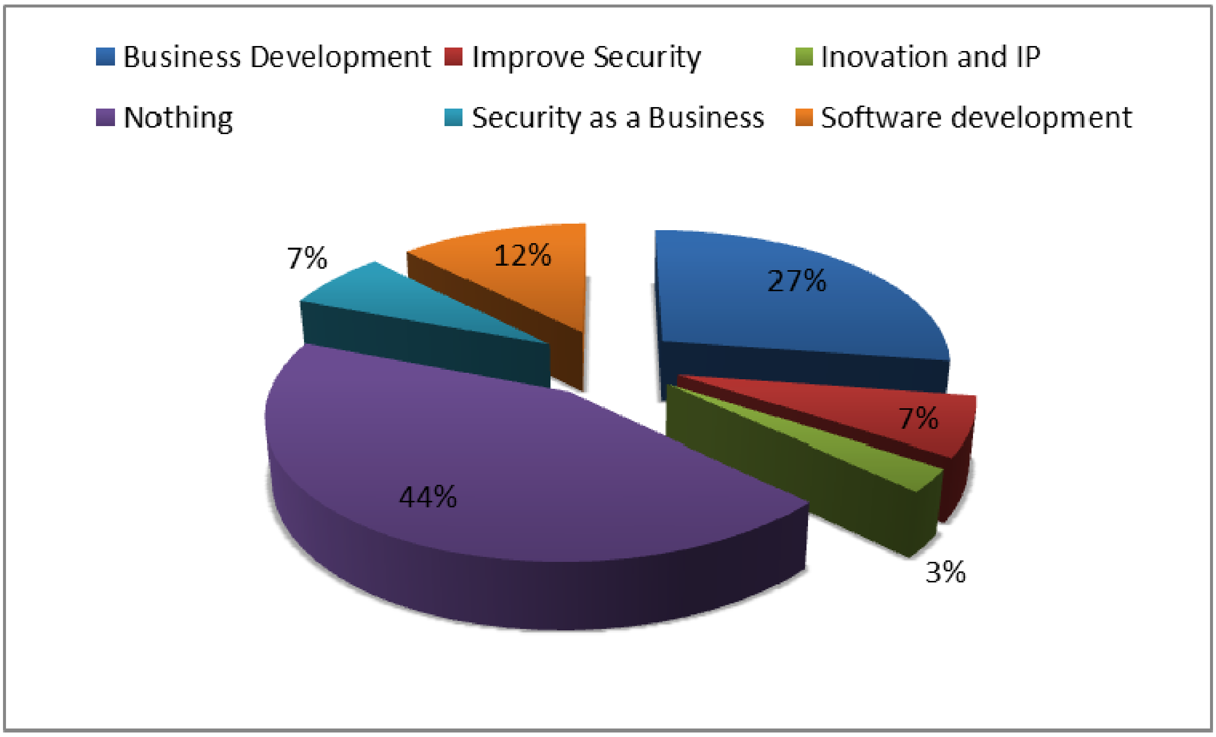

Figure 7 Registrants Response To Growth Aspirations By Percentage

### Growth Inhibitors

Given an understanding of what aspirations the companies have which are currently blocked, the registrants were asked the following question in order to elicit what they thought was blocking a successful out come to their aspiration.

**Do you feel there is a major issue stopping your organisation growth and if so what?**

The results of the question are given in Figure 8. The key inhibitors here are restrictions with regard to ‘finance sources’ followed by ‘Marketing capability’. With marketing capability a considerable number of respondents highlighted that it was difficult to get across to customers that there was a need for cyber security in products and services, despite the current level of government concerns. Although the majority of the registrants have a well defined problem space with appropriate solutions there appears to be a considerable concern that the message is not getting across. As a result the companies are spending much of their time identifying the problem space to their customers, in terms of their legislative responsibilities for example, before the solution can be identified. Unfortunately, this plays into the perception that many security vendors sell Fear, Uncertainty and Doubt (FUD) which cannot be relied upon as there is a clear incentive for the company identifying the problem space. There is a clear need for a better, independent awareness campaign in regard to the cyber security message which companies providing cyber security products can point to.

Interestingly the data show there is little correlation between those that wish to improve security and establish security as a business with the inhibitors of current security capability or security advice. The implication here is that what is stopping companies from diversifying and differentiating is money, lack of customer awareness and regional cyber security skills.

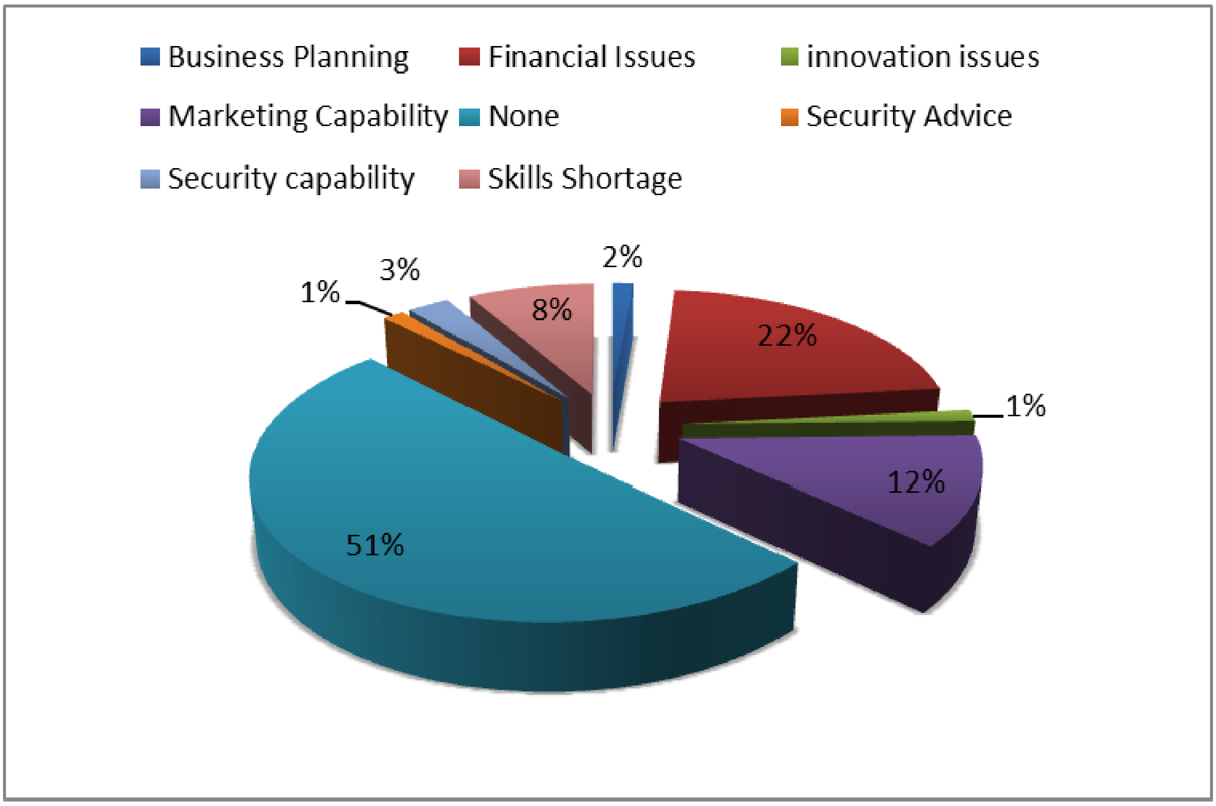

**Figure 8 Registrant Response To Growth Inhibitors By Percentage**

### Assistance Required

The opportunity was also taken to explore what specific advice and support the registrants felt they need in order to better protect their business in the current economic environment. Here the registrants were asked the following question:

**What assistance would be most useful to you to help protect your organisation?**

This resulted in the data shown in Figure 9. The data show that 33% of the registrants would like specific security related advice, with general background knowledge the predominant requirement. Clearly there is a general market failure in providing this advice if nearly one fifth of all registrant companies to a cyber security conference are struggling with access to general cyber security information. Cloud Security, Penetration Testing and Systems Security were the next three main requested assists.

The registrants have a clear desire to be better informed regarding the security issues surrounding current and emerging business processes and practices, both in terms of business considerations and technical understanding. However, the registrants are struggling to gain access to such information which appears to highlight a clear market failure of impactful, independent, reliable cyber security information.

As such, there is a clear need to determine the exact nature of the information required and how best to package this in order to maximise its exposure to the business community. Clearly in this case the existing resources must be identified and examined in order to identify where information is available and why it has not penetrated the marketplace in order to avoid the same mistakes.

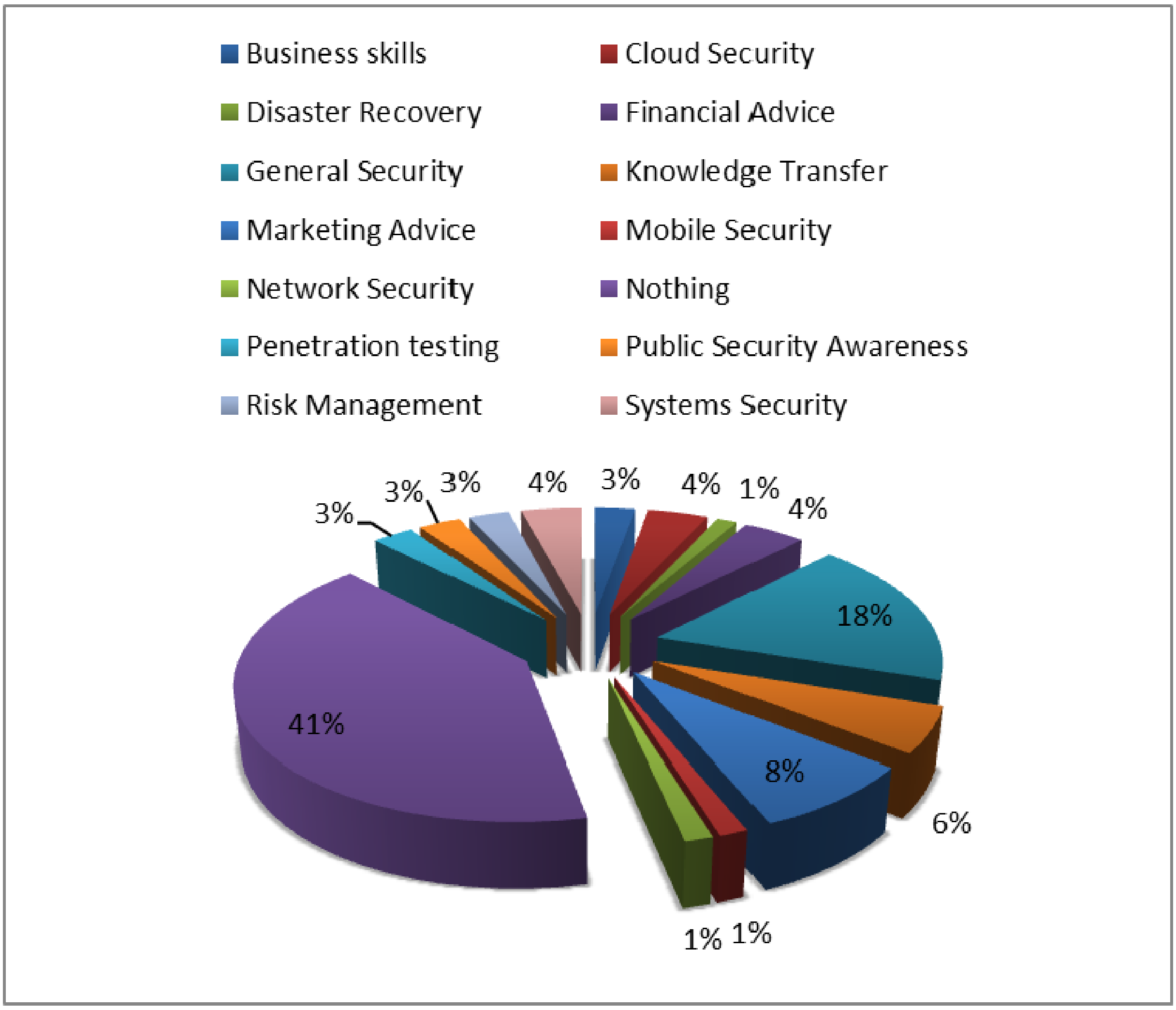

**Figure 9 Registrants Required Assistance to Help Protect Their Business**

## Phase Two: Technology and Cyber Security Survey

Phase two provided a more focused examination of the security and technology related issues that respondent companies might be facing. The Authors combined the data from Phase one with that of Phase two in order to provide the capability to compare business population factors to responses relating to security and technology related issues. Given that only 47 responses could be considered in this area a breakdown analysis of responses against business population information produced quite low numbers. As a result, whilst providing information of interest, it could not provide data with any statistically high level of confidence.

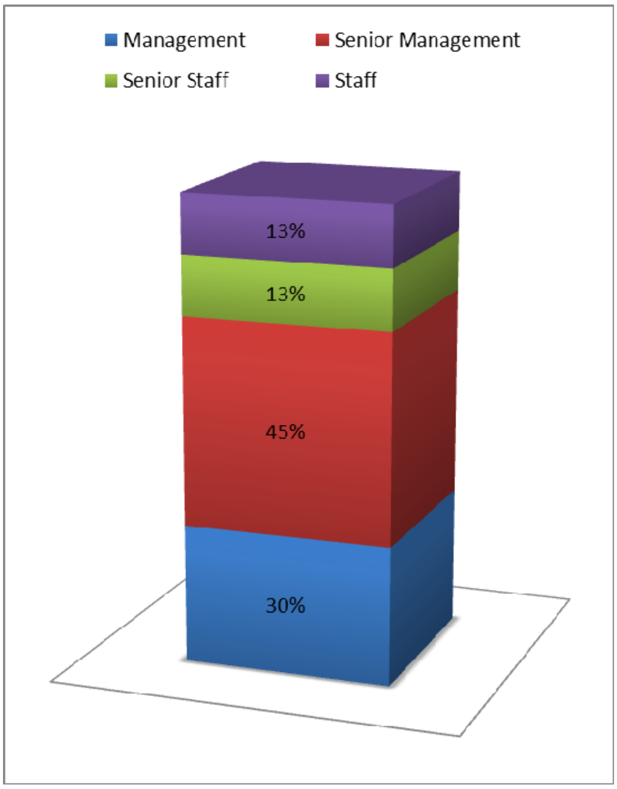

Figure 10 Respondent Role Classification

The role titles of the respondents were subjectively classified as either: Senior Management, Management, Senior Staff, and Staff, with the breakdown of respondents given in Figure 10. Due to the nature of the selection process in Phase One there is a clear bias towards senior roles in the respondents. This gives the Authors confidence that the collected data is from a suitably senior source as to be a representative set of answers to the survey questions.

The survey was broken into two main sections, the first part examines the respondents' attitude towards technology and policy and the second part examines the respondent's experience of cyber security issues. The second part is closely aligned with the survey approach adopted by ISBS2010 and ISBS2012. Where relevant data is available from these surveys appropriate comparisons will be drawn.

The results from this phase of the survey gave a mixed bag of good and bad results. While the respondent businesses broadly adopt new business models they fail to back this up with suitable protection. There is also a significant lack of translation from willingness to action within the security area and a lack of clarity of the nature and cost of the security incidents that companies face.

While the industry generally believes that the supply chain is a problem, these concerns are not being felt by the respondents to this survey. Generally many of the data sets that were collected through this survey are broadly in line with those collected by the national ISBS2012 and 2010 report. This enable comparisons to be drawn and demonstrates that security impacts all businesses in similar ways regardless of region.

## Part 1: Technology and Policy Attitude

The technological underpinnings of business are fundamental to its success in today's digital world. Therefore, an understanding of the way regional businesses utilise technology and approach technology use as part of their business process is vital to understand their cyber security concerns.

Enabling technologies for business are often considered as stable and part of a consistent reliable infrastructure. The Micro nature of the respondents would lead you to believe they would be early adopters of technology. However, the results in Figure 11 indicate otherwise. Although the adoption of remote access technology is similar to the data reported in ISBS2010 (data for 2012 was not available), the region lags behind in wireless (ISBS 2010 85%) and virtualisation (ISBS 2010 69%) adoption despite the rapidly decreasing cost of these technologies. The attitude towards virtualisation is understandable considering the Micro nature of the respondents, i.e. there is no need to virtualise their systems. However, the prevalent nature of wireless technology makes it strange that the respondents would have such a difference. The conclusion drawn was that the nature of the audience, self-selecting security enthusiasts and professionals, would have a tendency to avoid perceived insecure technologies such as wireless. Also worth noting is the significant adoption of VoIP technology in comparison to ISBS2010, which reported only 47% penetration.

**Which technologies does your company use to enable business?**

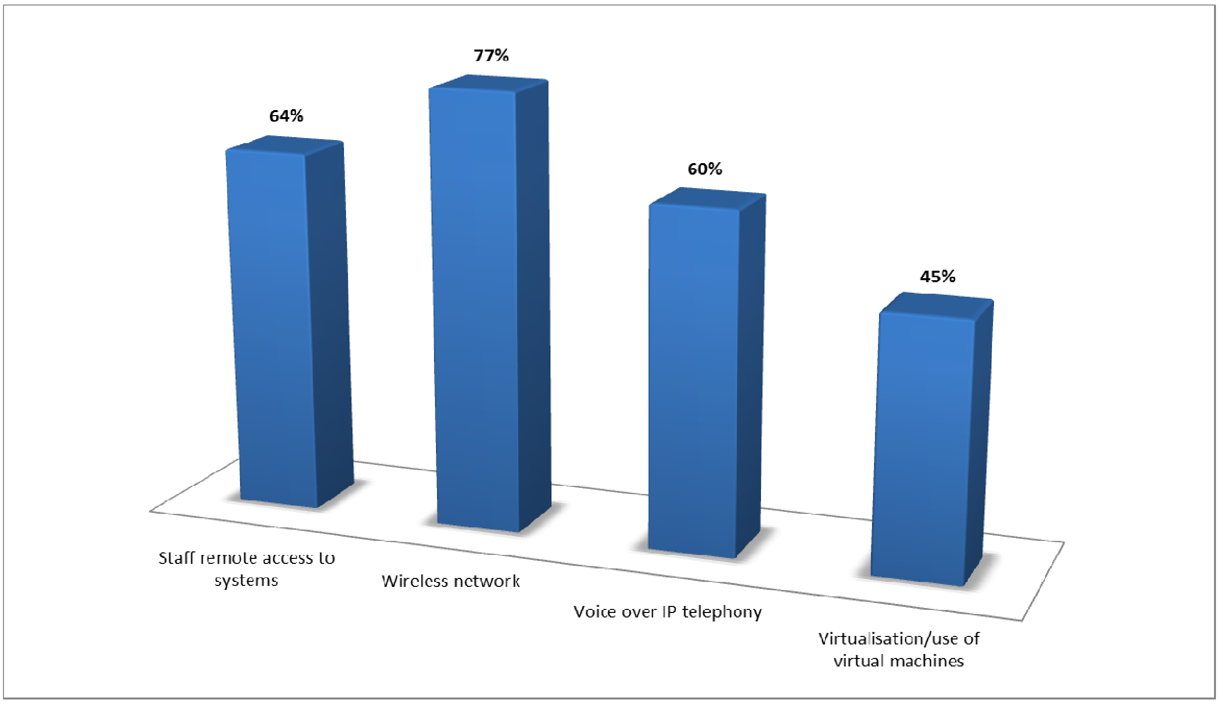

Figure 11 Business Enabling Technologies

This research reveals a number of key considerations. Importantly the respondents have poor protection against security failures of out sourced business process despite significant adoption of the outsourcing model. In addition to this there is significant executive level of concern, and yet this does not translate into action on security issues. Further there is a lack of compliance requests across the supply chain; however, protection of the customer is the main driver for security expenditure. These, high level outcomes help to formulate an appropriate response in order to support regional businesses.

## Outsourcing Services

Another key approach to enabling business is the outsourcing of elements of the business process to 3rd party service providers. A total of 68% of the respondents had outsourced some of their core business functionality externally. Broadly the responses to this question are in line with those reported in both ISBS2010 and ISBS2012 as given in Figure 12. There is a noticable tendance for the respondents to be more reliant on some main business functions. The Authors again suspect that the Micro nature of the respondents are the cause of this as it is represents a lower cost to the business in terms of support and licencing.

What is troubling given the increased reliance on outsourcing is the respondents lack of appropriate mechanisms to protect themselves in key areas from failure in the provider as shown across in Figure 13. In this analysis the sample size is reduced to only those respondents that have outsourced a service. Only 59% of all respondents who have outsourced have put in place any form of protection. The most popular protection mechanism is through contracted provisions at 47% which is much higher than that reported in ISBS2012 (36%). Importantly the respondents are much worse on obtaining audit rights over the supplier and most significantly have an exit strategy for when the provider withdraws the service, with only 9% having something in place compared to 41% in the ISBS2012 report.

Clearly work needs to be completed in this area in order to provide advice to business regarding how to safe guard their cloud based service provision for customers. What was not explored in this survey is the nature of the data that was kept in the cloud, beyond the obvious association of data types with the services provisioned. This will be an area of future analysis in subsequent surveys.

**Have you outsourced any of the following business processes to external internet based providers?**

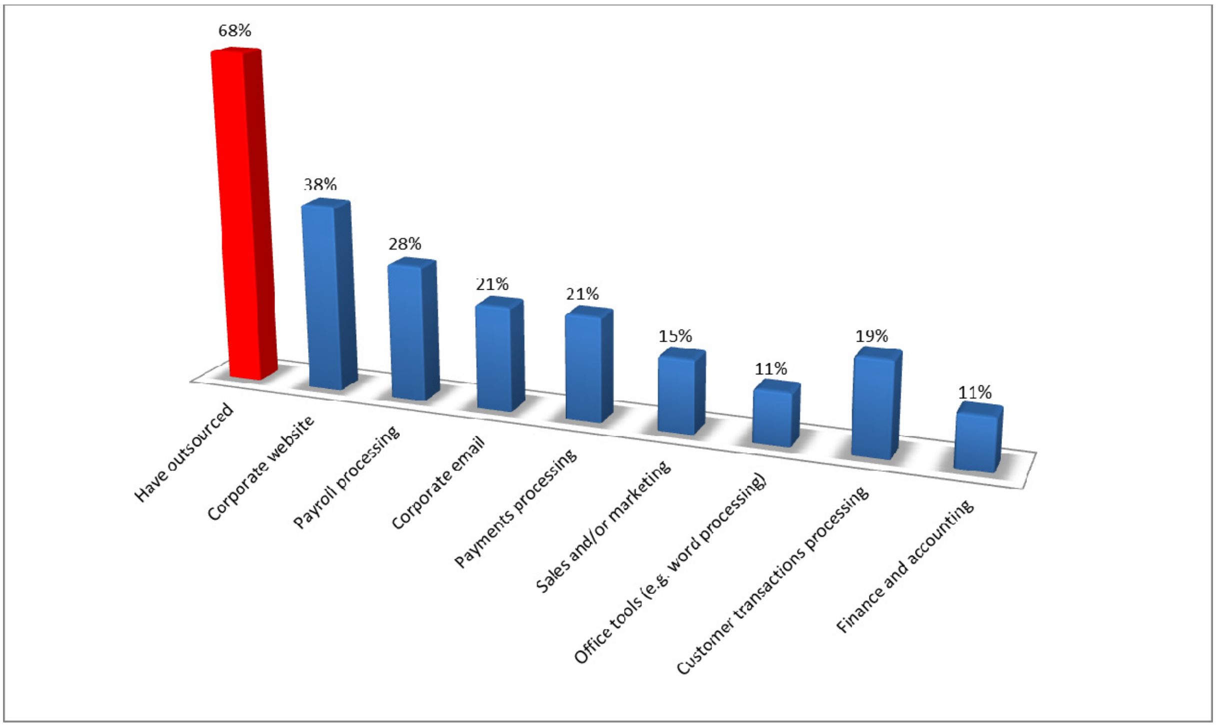

**Figure 12 Outsourced Services**

**If you have outsourced any element of your business processes, have you taken any steps to ensure the security of the external services provider?**

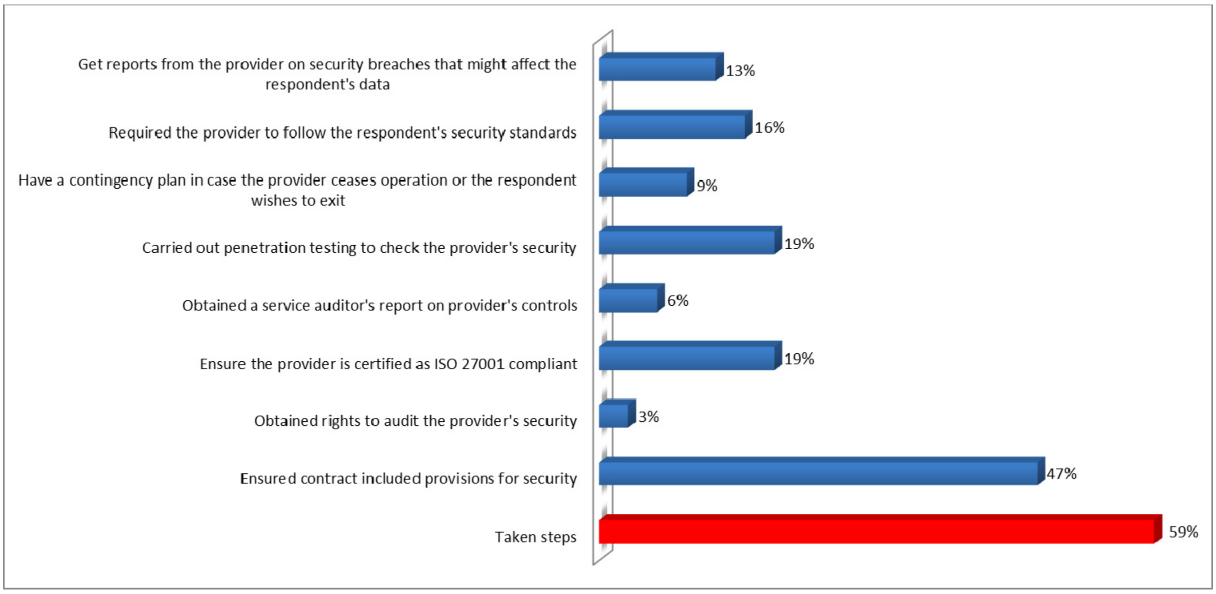

**Figure 13 Outsource Security Measures**

These technology trends indicate that digital integration of businesses is significant with a highly mobile workforce leveraging cloud based services to enable productivity and new versatile ways of working. One explanation for this could be the sparse nature of the population in the Lancashire and Cumbria regions coupled with excellent transport links to major population and business centres which demand a mobile workforce in order to conduct business. It is clear that there is significant adoption of outsourced services by the respondents. Further analysis is required in order to understand the motivations and rationale behind the respondents outsourcing their business processes in order to better understand the risk/reward tradeoffs.

## IT Security Policy

One of the main drivers for information security operations is the policy that the company has in place. A comprehensive policy covers all aspects of information security from data classification to management process, and embodies the principles of operation. The policy is then enacted as a set of guidelines or standard operating procedures.

The respondents clearly consider cyber security to be a high business priority with 98% of them indicating that IT security is a high or significant priority. This is again a natural result due to the nature of the respondents having also registered for a cyber security conference. This response profile is broadly in line with the data from both ISBS2010 and 2012.

What is troubling however, is despite the clear priority for IT security displayed in Figure 15, coupled with the senior profile of respondents as reported in Figure 10, it seems that this senior sponsorship does not translate into action. As can be seen in Figure 14 only 43% of the respondents actually have an IT security policy in place, despite the policy being the bedrock of business support in this area.

**How high a priority is IT security for your company?**

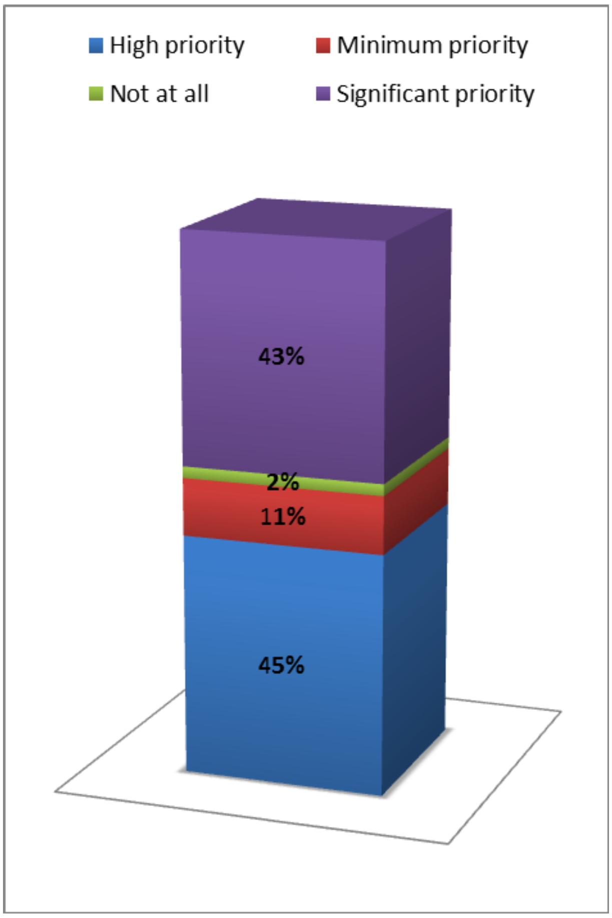

Figure 15 Security Priority

**Do you have a formally documented IT security policy?**

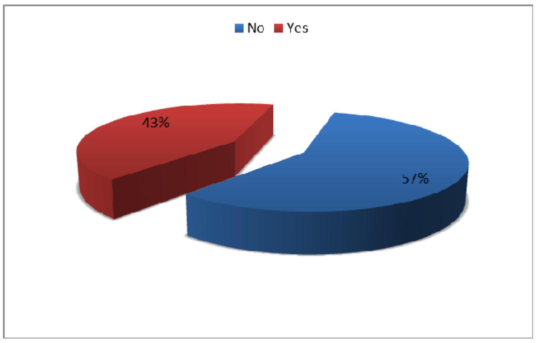

Figure 14 Formal IT Security Policy

This lack of translation from willingness to action is a significant issue specifically for Micro enterprises, where a security breach and the associated cost of recover, direct and indirect loss could cause the business to financially collapse.

There clearly needs to be an actionable framework that senior business stakeholder can employ in order to support this translation. While some frameworks do exist, the reason for their adoption is unclear and could range from a lack of education to the frameworks being too complex. Further analysis is required to understand this lack of adoption.

## Staff Awareness and Education

Awareness and education of staff with regard to cyber security issues represents the front line in preventing successful cyber security attacks. It is regularly reported by analysts that social engineering attacks are on the rise. It is clear also that these attacks are becoming more sophisticated and automated. The emergence and continued development of the Social Engineering Toolkit (SET) (David Kennedy, 2012) is one example. This toolkit provides an easy to use platform to automate the creation of phishing attacks, spear phishing attacks, fake websites, and compromised removable media. The framework utilises Metasploit (Metasploit, 2012) ensuring that the latest technological attack vectors are available to the malicious attacker.

**How do you ensure your staff are aware of IT security threats?**

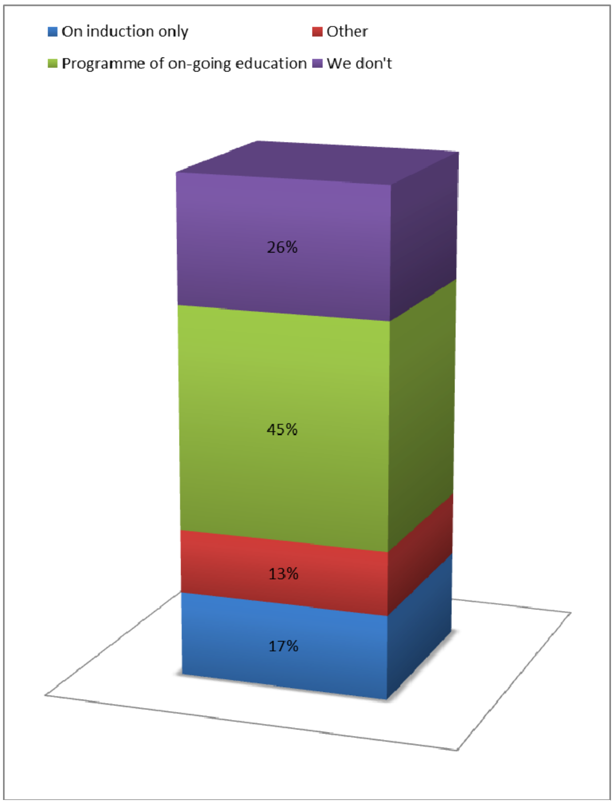

Figure 16 Staff Awareness Education

However, it is not just the 'malicious outsider' that companies need to be aware of but also the unknowledgeable accidental insider that could act as a threat agent and breach a company's information security responsibilities. It is for this reason it is great to see that 45% of companies have an ongoing education programme to help educate their staff. Overall three quarters of the respondents provide some form of security education, yet nearly 20% only provide this education during induction and seemingly leave it up to the employee to educate themselves from their peers and other sources. The figure for ongoing education is in line with ISBS2012, however, the respondents to the ISBS2012 survey did better in terms of their indication as 31% provided cyber security training as part of their induction.

**Are you/your staff aware of government legislation regarding the holding of/disclosure of confidential information?**

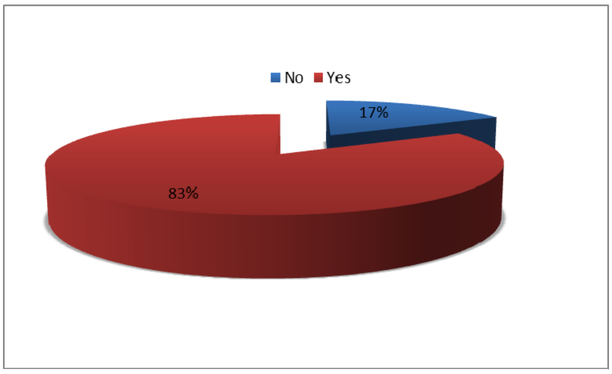

Figure 17 Staff Awareness of Data Legislation

Figure 17 shows the split of whether the respondents felt that they or their staff were aware of appropriate legislation regarding the holding and disclosure of confidential information. On the face of it the response appears to be strong, with 83% saying they are aware of all appropriate legislation. However, there is a methodological problem with this question as it is ambiguous as to whether it is referring to the respondent or their employees. Therefore, the readers should adopt caution in reading too much into this data and it is only provided in this report for completeness and to provide an indication of where the respondents feel they are in this aspect.

In future surveys care will be taken to separate out two considerations. Further questions will also be asked in order to provide a quantitative approach to assessing respondent knowledge, rather than subjective self assessment. Overall there is good work being done in the region with regard to user education. In addition to the more nuanced line of questioning, future surveys we also explore how the respondents measure the effectiveness of their training and the potential impact on the business if they are seen not to be providing such training.

## Compliance in the Supply Chain

Both ISBS2010 and SBCSS2012 reported a focus from all points in the supply chain on compliance. As with social engineering, the security of the supply chain is a significant concern to all sectors. Attacks on smaller companies less able to defend themselves provide an easy route into larger organisations via the digital integration that underpins modern business.

The security of the whole chain is only as strong as the weakest link in terms of the technology, people and process they have in place. However, it should not be considered a big to small issue. Smaller companies should be just as concerned with what is occurring in their supply chain, particularly when they are consuming vital business services from larger organisations.

Many standards that are commonly used today do not allow a company to pass the buck for a failure down the supply chain. If a company suffers a breach because of another company, potentially they are just as culpable as the company who created the situation where the breach conditions occurred originally as they have not followed suitable duty of care procedures for their data. For these reasons we queried the respondents on their perception of requests for compliance from their customers and suppliers and partners as can be seen in Figure 18 and Figure 19.

**Have any of your customers asked that you comply with any of the following guidelines in the last 12 months?**

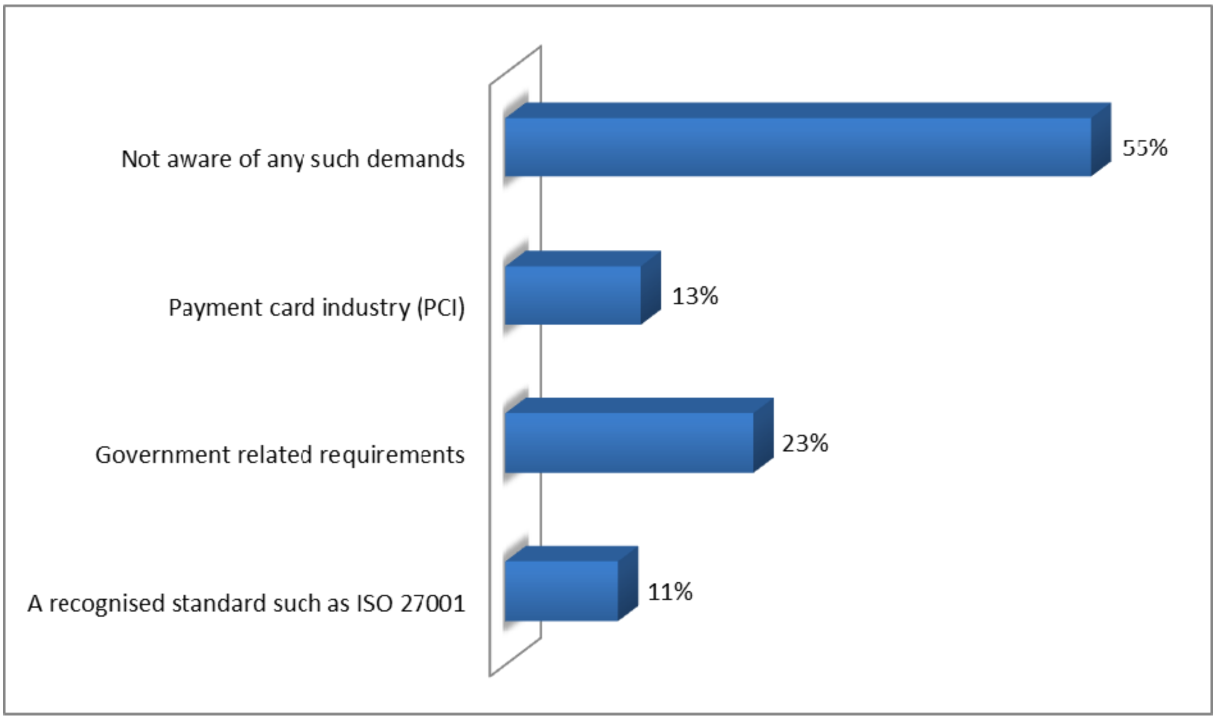

**Figure 18 Request from Customers for Compliance to Standards**

By comparison to the ISBS2010 survey it would seem that the respondents' customers are not very demanding with regard to compliance. This is surprising considering the nature of the large industry in Lancashire and Cumbria, including critical national infrastructure and defence services. However, the respondents report request levels well below those in ISBS2010, in some case less than a third, and significant lack of demands. It simply cannot be the case that respondents customers are all consumers as there were few respondents identifying themselves with direct consumer facing activities such as retail so perhaps one explanation is that the small size of the companies taking part in the survey means that they are so far along the supply chain that these types of demands have not been filtered down to them. Future surveys will attempt to explore the supply chain mapping and critically analyse how the business interacts with their supply network. Through this collection of data the Authors hope to be able to obtain a more nuanced understanding of a representative supply network model for different sized regional businesses so as to help companies understand the potential risks they are exposed to.

## Have any of your suppliers/partners asked that you comply with any of the following guidelines in the last 12 months

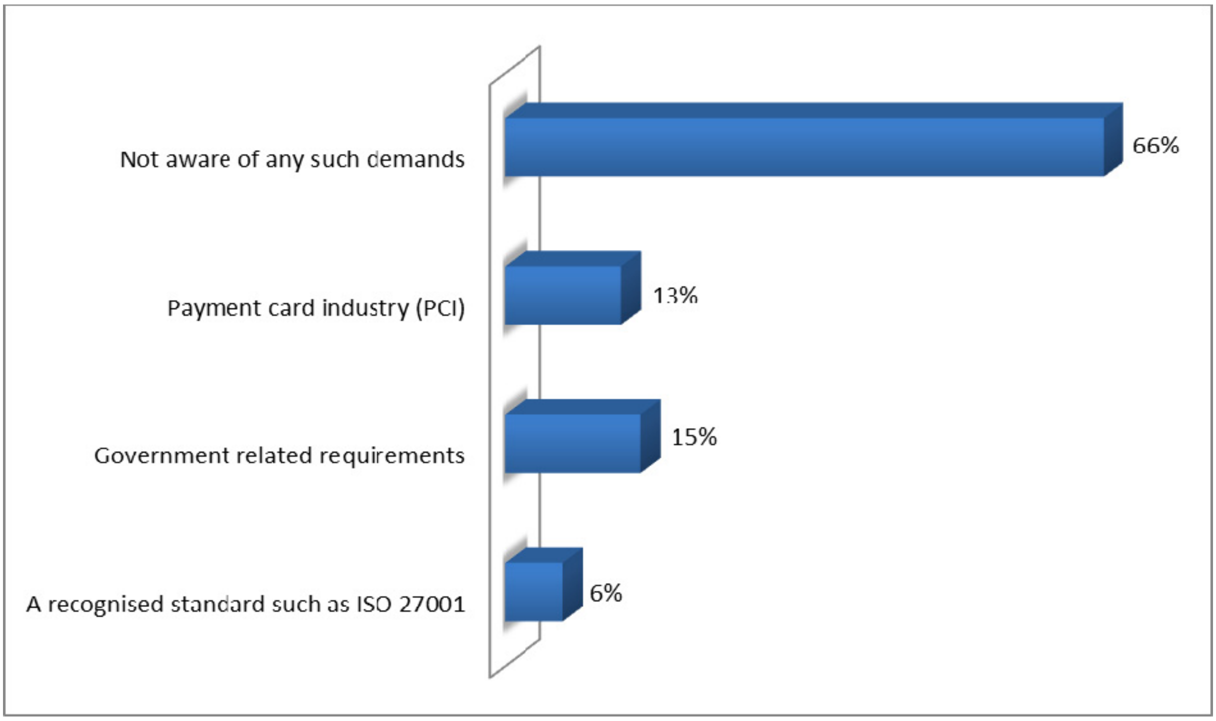

**Figure 19 Requests by Supplier/Partners for Standards Compliance**

The survey also asked if they had been asked by any of their suppliers or partners to comply with standards in order to understand if their downstream links in the supply chain were placing demands on them. There is a more severe picture here with even less requests being issued. There is no direct comparison for this data in related surveys.

This data, coupled with the information regarding the demands placed on their providers, shows a generally lack of demand for compliance across the supply chain. It is not clear as to whether there is an underlying cause to this lack of demand and whilst the Authors have provided some possible explanations through the previous section of text, to answer these issues in more in depth an more comprehensive analysis of the supply chains in practice needs to be carried out. The Authors suspect the security considerations of any approach is based around identifying and minimising risk to larger partners and putting in place a punitive set of measures for any infringement. However, this needs to be confirmed by further polling and analysis.

## IT Security Budgets and Expenditure

### What is the main driver for any IT security expenditure you make?

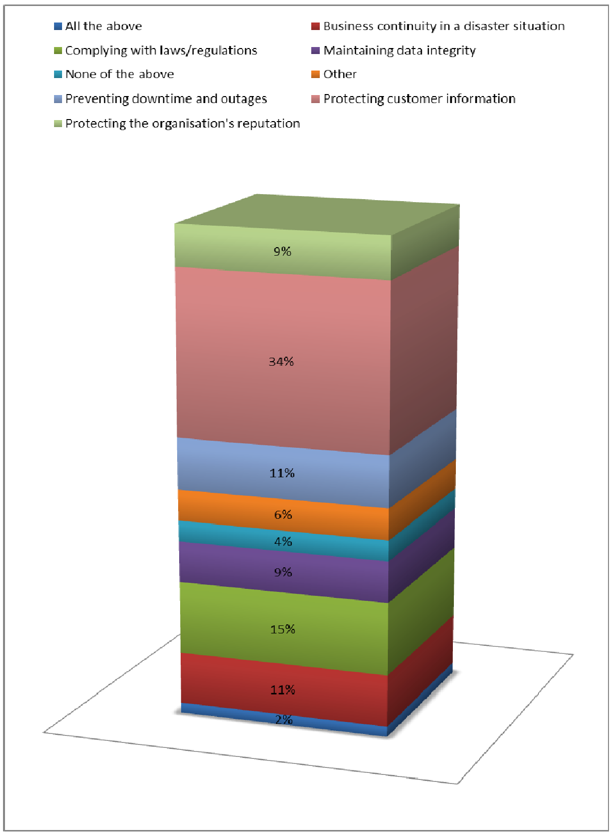

Figure 20 Main Driver for Expenditure on Security

There are clear motivations for spend on information security from compliance and legislation requirements through to conscientious business practice. Understanding the motivation for this spend provides a key insight in a business's approach to cyber security and indicates how the respondents feel about it, as a cost or as best business practice. The analysis of the data shown in Figure 20 indicates the top four drivers are; protecting customer data (34%), Complying with Laws and regulations (15%), Business Continuity (11%) and preventing downtime and outages (11%). The top three are exactly the same as that reported in ISBS2012, with the proportion of respondents being nearly identical.

Overall therefore there is a positive bias towards putting the customer first as a strong business strategy, followed strongly by protecting the business itself. How this recognition of the importance of expenditure on IT Security is translated to actual spend is addressed in the next question.

### Roughly what percentage of your IT budget, if any, is spent on information security?

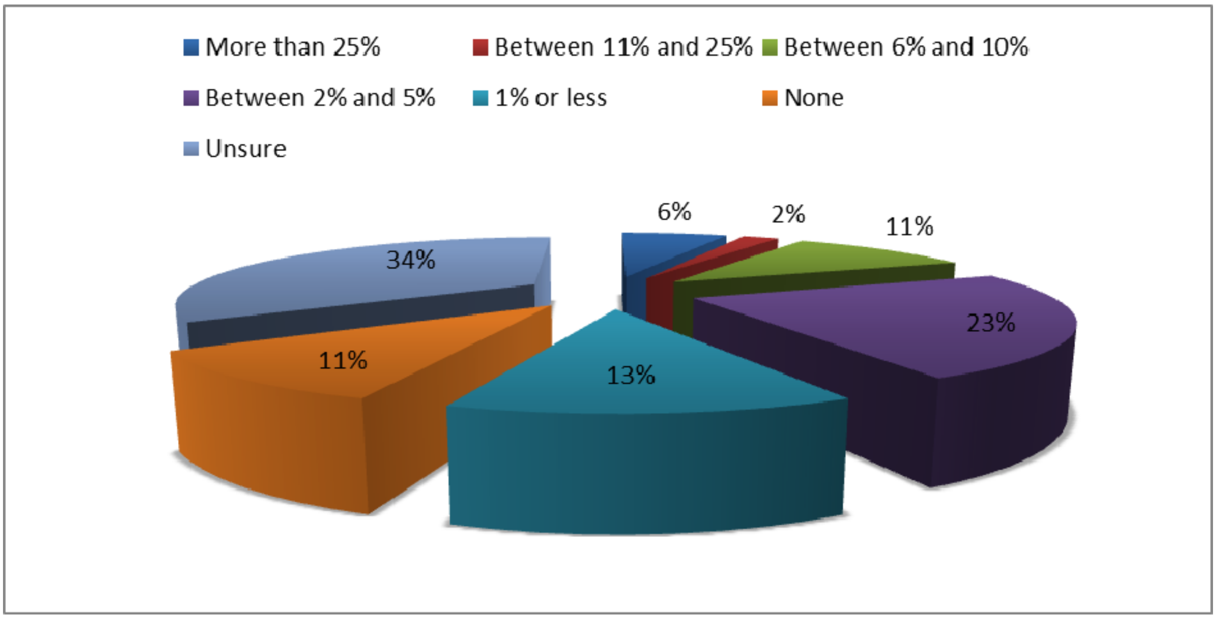

Figure 21 Percentage of IT budget Spent on Information Security

As was previously reported earlier in this document, again, the high priority attributed to Cyber expenditure does not translate into action. It is clear from the data in Figure 21 that while the respondents are comparable at the higher end (SB-CSS2012, 6%/ISBS2012, 4%), there this a significant slump towards the lower end of expenditure with ISBS2012 reporting 34% spending less than 5% in comparison to 47% for this survey.

The combination of data from IT security policy uptake and security expenditure highlights that there is a systematic issue in taking willingness and driving action. What is not clear is the driver for this lack of translation. There are two primary hypothesises in that the Authors would advance. Firstly, although it is a concern the primary drivers in the demographic are to start up and survive. This necessitates a focus on the core business model which would then adopt security practices later if the business survives, which is the norm. Alternatively, there is not the advice or guidance available in order for companies to easily translate willingness into action in a cost effective way.

In future surveys it would be interesting to explore how companies measure the impact of their expenditure and how they currently make their decisions regarding funding allocation. This will expose the feedback loop in the decision process by which businesses plan information security expenditure.

## Part 2: Cyber Security Incident Experience

**In terms of incidents what are you expecting in the future?**

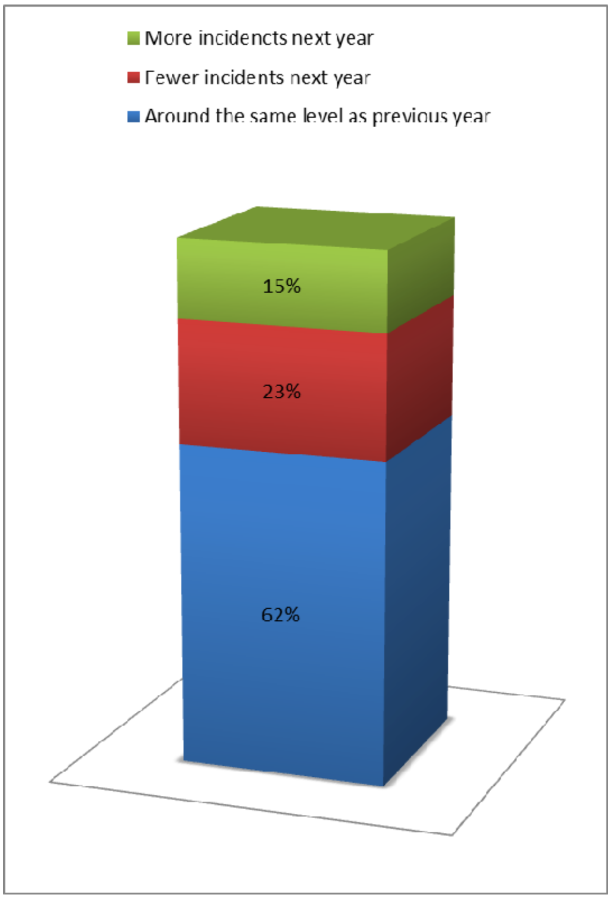

**Figure 22 Expected Future of Security Incidents**

The second part of the survey examines the respondent’s experience of cyber security incidents by investigating the type, nature and impact of the events they have experienced. The respondents were initially asked how they felt the future looked in regard to security incidents.

Overall the respondents were quite buoyant about the future, with 85% believing the number of incidents would be the same or better in the next year. The majority of respondents (62%) were expecting a similar future to what that they have experienced previously.

This is a common response to this type of question where respondents tend to predict what they have experienced in the past, it is generally those that have suffered an incident that tend to learn from that experience and become more pessimistic. This type of “Black Swan” (Taleb, 2010) thinking is prevalent in security thinking generally.

In essence, and to quote, Monty Python, “nobody expects the Spanish Inquisition!” However, whilst incidents are by their very nature unpredictable that cannot detract from the fact that they do still have a probability of occurring, and in this highly connected digital world where physical distance is not a significant consideration everyone can be a potential target. It therefore should be a question of not ’if’ but ‘when’ and businesses need to consider their defensive and response capabilities. Given this assertion that it is those companies that have suffered and learnt from an IT Security incident that are by far the most likely have a realistic viewpoint of IT Security then it would be reasonable that this groups are also more likely to implement reasonable security practices. Taking this into account, the key challenge must be how to give companies that more realistic viewpoint on the nature of IT/Cyber risk to them without having to expose them to that initial incident.

In many of the responses, the data shows that typically 50% or more of respondents reply ‘no’ or ‘unsure’ to questions such as, “How much has this incident cost?” or “Have you suffered an incident of type X?”. The Authors are unclear as to how confident the respondents who answer ‘no’ can actually confidently say no or whether they are really unsure. This area needs to be explored in more detail in future surveys. However, overall this is a worrying trend where the respondents are not clear as to the types of incidents or the costs associated with them. The profile for malicious external attack responses is similar to that of ISBS2012 and demonstrates that this region is not immune to a national trend. The single most significant security incident type is that of System Failure or Data Corruption, providing a clear case for business to look at appropriate business continuity plans and practice accompanied by suitable disaster recovery planning. The cost of recovery from a security incident is generally reported to be sub £10k. However, the data show that many of the respondents do not assign a cost to the recovery of the incident, however, clearly there must be an associated cost in order to respond and recover systems in terms of staff time and replacement equipment.

## Security Incidents

IT Security incidents can range from an unintentional and accidental data leakage from a member of staff to a targeted malicious external attack and everything in between. The respondents were queried on the severity and the type of incident with an exploration on the frequency of their discovery of malicious software attacks. This analysis facilitates a better understanding of the nature and severity of the incidents in order to provide appropriate response mechanisms.

The classification of the incidents the respondents have suffered is documented in Figure 24 below. Here it would appear that the majority of the specific incidents are minor with a roughly 50/50 split between accidental and malicious. One tenth of the respondents suffered what they determined to serious malicious directed security incident.

More specific questions regarding the nature of the incident were then asked and the results are shown in Figure 25. When compared to ISBS2012, it would appear that the respondents are doing well with considerably lower figures across the board. However, 13% of respondents did state that they were ‘unsure’ which would appear to indicate the question assumes a higher level of technical knowledge in the respondents than was perhaps evident. Potentially the data highlights that those companies that have responded with a detailed understanding of the type of incident have a level of sophistication in their ability to detect such events, rather than being representative of the actual number of breaches that have occurred.

## In the last year, have you had any of the following?

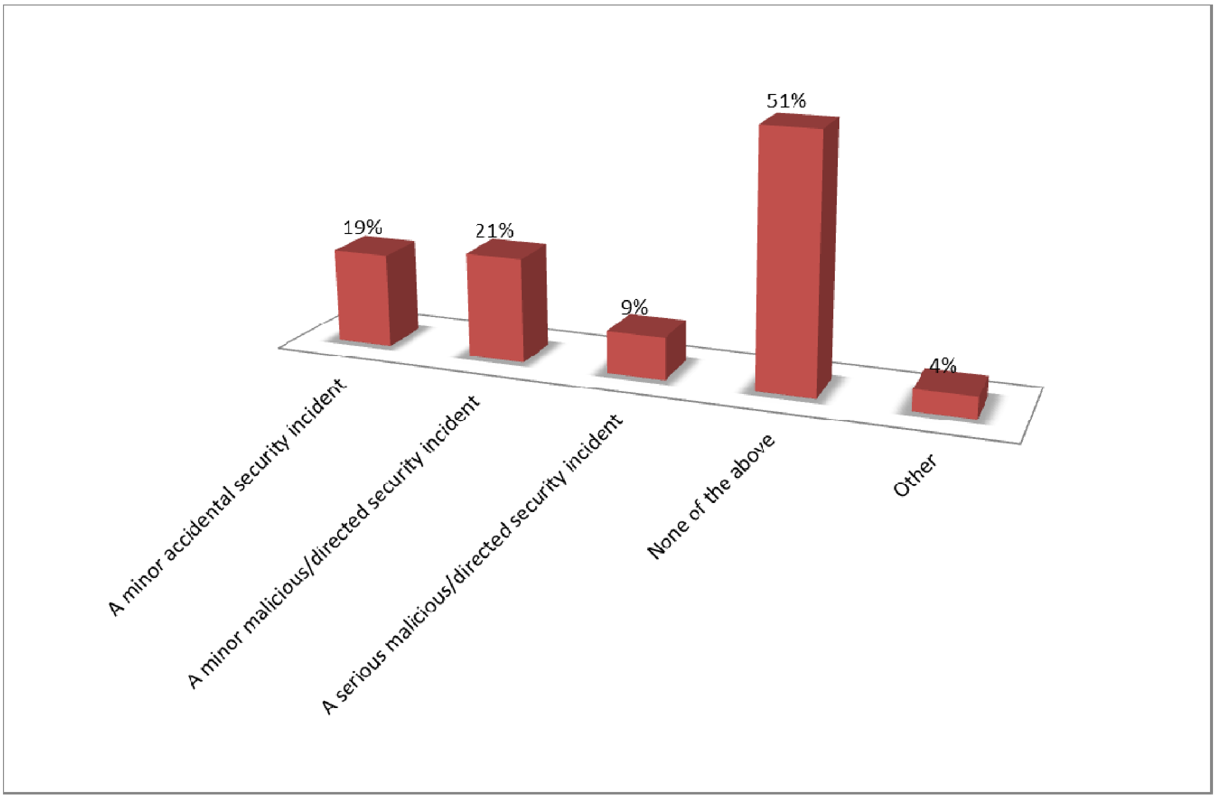

**Figure 24 Breakdown of the Types of Security Issues Suffered in the Last Year**

## What type of security issue have you suffered, if any?

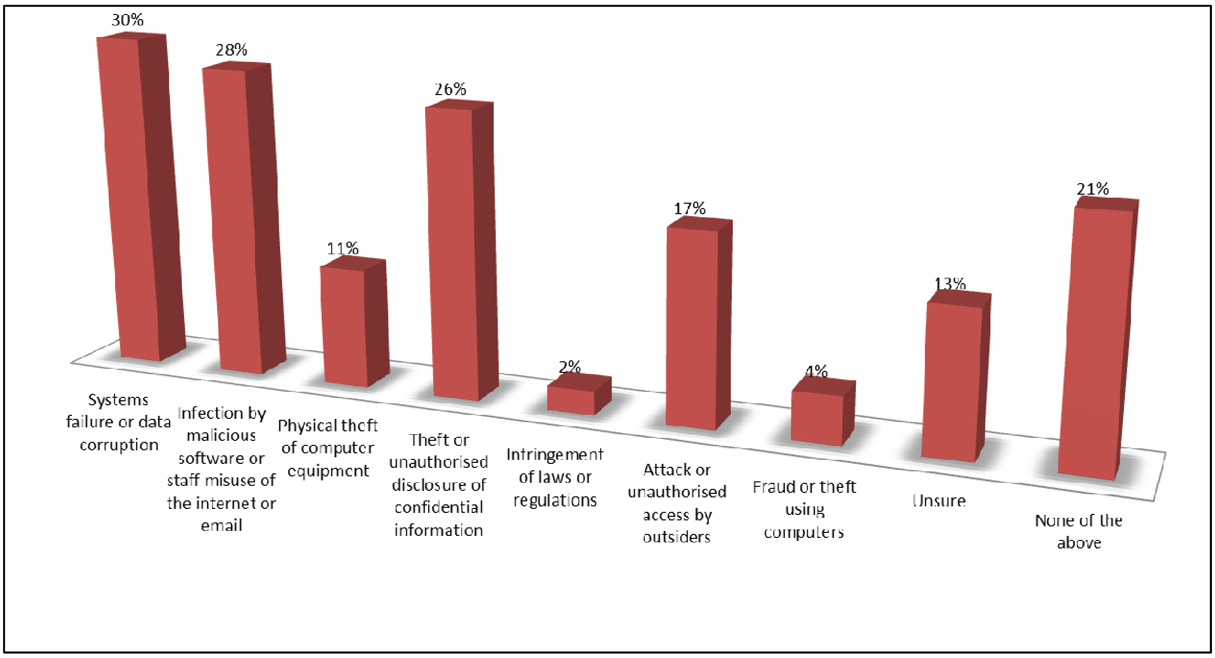

**Figure 25 Types of Security Issue Suffered**

Respondents were initially asked about the nature of any security issues they had faced and then a cross referencing exercise was completed to see how respondents considered the severity of the nature of the event. In the responses to the questions it was possible to select multiple categories to each answer. In terms of severity there were only two such instances so there is the potential for the severity in the classification of the nature of the incidents to be over/under inflated. The initial responses can be seen in Figure 24 with Table 4 and Figure 26 detailing the cross referenced data.

The information in figure 24 demonstrates a strong skewing of the results due to the inclusion of a catch all "None of the Above" response. This confirms the Authors opinion that a more detailed series of categorisation is required to better understand this domain. What can also be determined from the cross-correlated data is that respondents consider the majority of the incidents, regardless of their nature to be minor. One additional factor that was seen in the correlated data was that a large proportion of systems failure, theft and infection was largely unclassified in terms of severity. This information is of interest in that it may give insight in to why companies may not be allocating significant portions of their IT budget to information security.

| | **Systems failure or data corruption** | **Infection by malicious software or staff misuse of the internet or email** | **Physical theft of computer equipment** | **Theft or unAuthorised disclosure of confidential information** | **Infringement of laws or regulations** | **Attack or unAuthorised access by outsiders** | **Fraud or theft using computers** | **Unsure** | **None of the above** |
|---|---|---|---|---|---|---|---|---|---|
| **A minor accidental security incident** | 4 | 3 | 1 | 3 | 0 | 1 | 0 | 2 | 0 |
| **A minor malicious/directed security incident** | 2 | 5 | 1 | 1 | 0 | 4 | 0 | 0 | 1 |
| **A serious malicious/directed security incident** | 2 | 1 | 1 | 0 | 0 | 3 | 1 | 0 | 0 |
| **None of the above** | 6 | 6 | 2 | 8 | 1 | 1 | 1 | 3 | 9 |
| **Other** | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |

**Table 4 Incident Classification By Incident Type**

One particular incident type that is noteworthy and one it would appear that respondents have a sophisticated interpretation of, is that of 'Infection by malicious software. Here, respondents appear much more able to define the severity of the malicious attack.

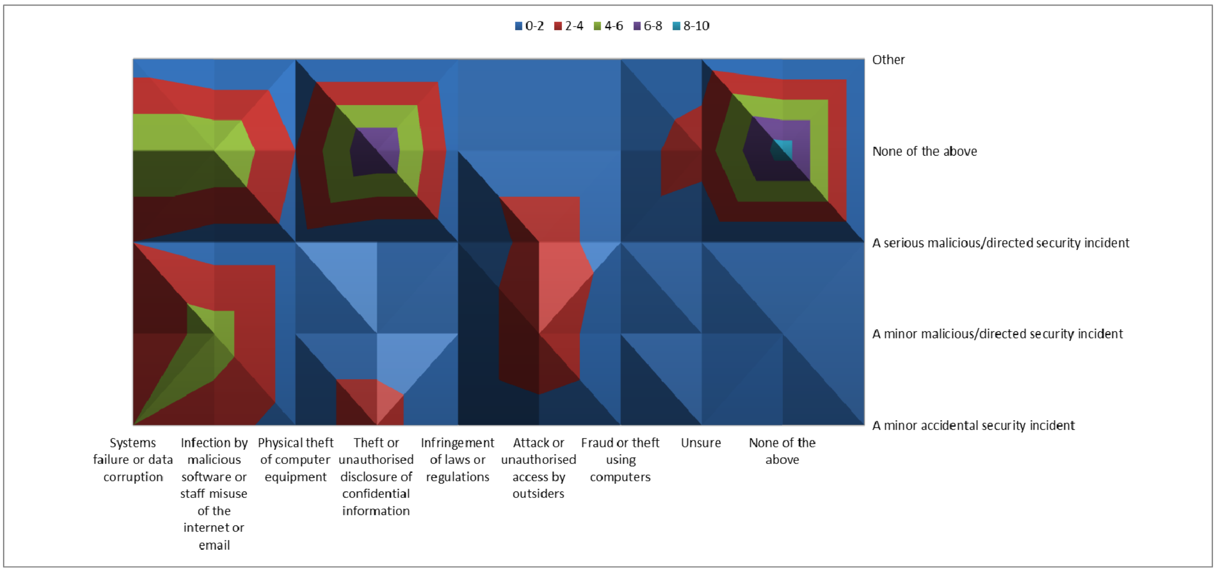

**Figure 26 Incident Nature Cross-referenced by Incident Severity**

Of particular interest to the Authors was the frequency of the events involving malicious software attacks. This information is representing in Figure 27. Tools for malicious software detection and removal are freely available and arguably the technology has reach a commoditised phase of existence with the cost of leading products approaching a zero cost. Most products also come with fairly straight forward reporting tools providing easy to interpret data sets at prices to suit all budgets.

Given the maturity this security product market it is therefore surprising to note that 13% of the respondents were unsure how many malicious software infections they had suffered in the last year. A full 30% of respondents also indicated that they had no incidents whatsoever. However, as with previous analysis it is not clear whether the respondents could definitively say that they had no infections or whether they lacked an appropriate level of sophistication to detect such events.

## How many malicious software infections do you think you suffered in the last year?

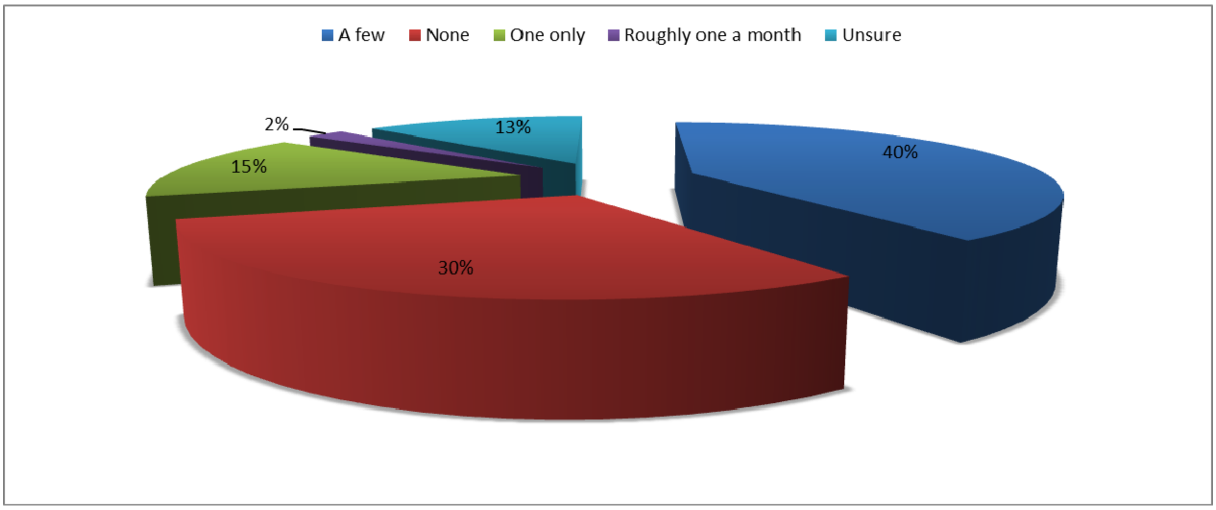

**Figure 27 Malicious Software Infections**

At a headline level the information gained in this survey shows a set of companies dealing with IT Security issues well in the face of a high level of attacks. However, the nature of the survey questions leaves this interpretation open to some degree of question as there isn't enough detail available to determine whether it is the case that there are actually no security events at all or whether it is more likely respondents just didn't possess the skills or awareness to detect the events. Further methodological alterations to the survey are required in order to probe these questions in more detail.

### Insider Incidents

**Have you suffered a staff related security incident?**

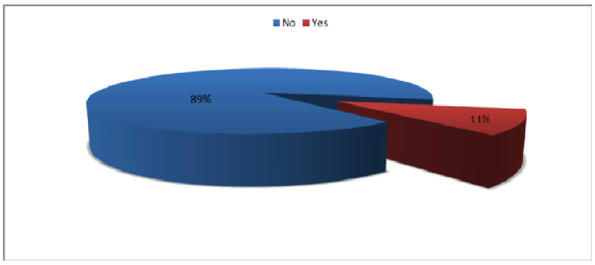

**Figure 28 Staff Related Incident**

As highlighted previously, the impact of insider threat can be very significant. Those inside the organisation have access to sensitive company data and are ideally placed to cause significant issues whether accidentally or maliciously. For this reason the survey explored the respondents' experience of this type of event the results of which are given in Figure 28.

The findings of this survey give a clear indication that staff related incidents are very low in respondent companies and much lower than the 45% figure reported in ISBS2012. Further investigation is required here and it is unclear whether respondents are significantly more aware of the issues concerned and whether those respondents that provided a "no" answer are confident in their assessment and have the capability to be able to accurately make that assessment. Further questioning of the "no" respondents in future surveys is required in order to understand this answer set more fully.

**If you answered 'yes', what was the nature of the incident?**

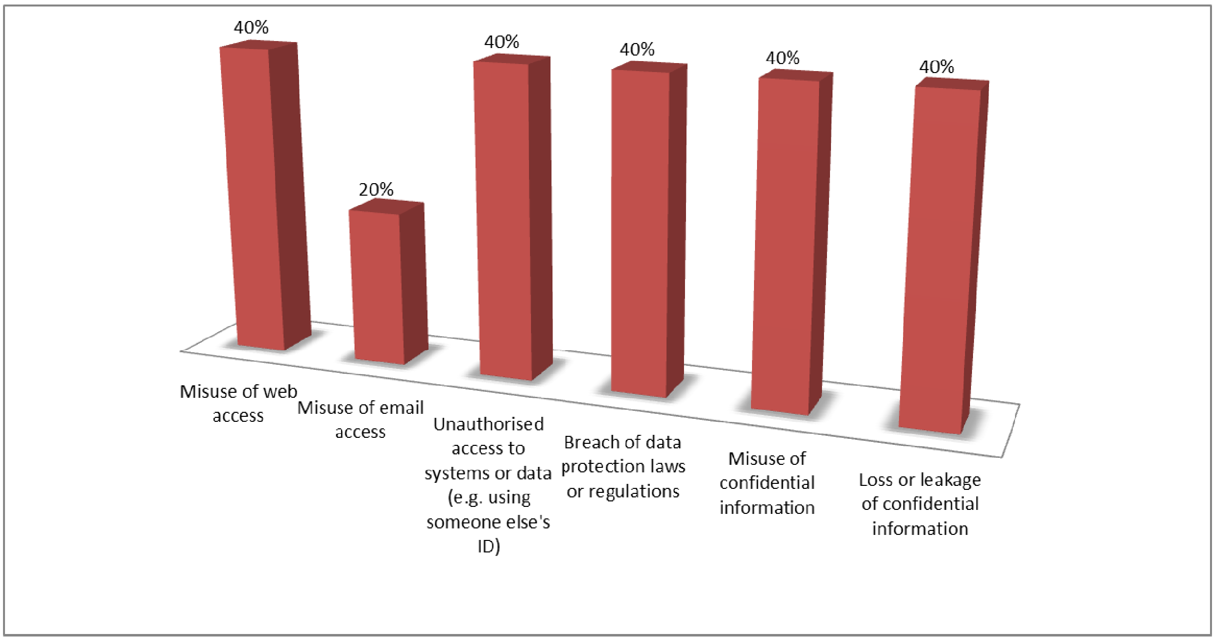

**Figure 29 Nature of the Staff Related Incident**

To explore the nature of insider threat in greater detail, respondents who replied affirmatively were then asked for further details as to the nature of the incident.  These findings are displayed in Figure 29. Caution must be taken in inferring too much from the data as the sample size of these results is reduced to six respondents and so cannot be treated as statistically significant. The results, while interesting are included in this document for the purposes of completeness and also, perhaps, to offer support a case for a much wider survey.

### Malicious External Attacks

Malicious external attacks are the IT Security event that every company fears and are arguably the one, alongside accidental data loss, that gets the most media coverage.

If we set aside the recurring question regarding the validity or reliability of the 'no' response, i.e. is it a definitive "no" or "I don't know for sure", worryingly nearly 20% of respondents are unsure whether they have been attacked by a malicious external party or not.

**Were your company's systems attacked by an unauthorised outsider in the last year?**

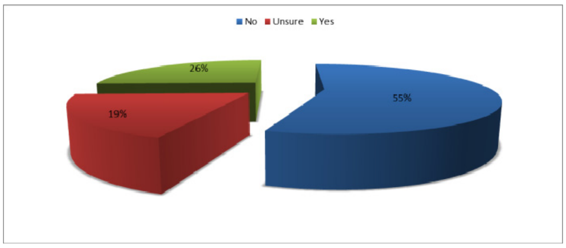

Figure 30 Malicious External Attack

While the intrusion detection market is not as mature or as penetrating as the anti-malware space, there are a number of products available that would be able to identify an external attack taking place.  However, the lack of awareness may also be compounded by the extensive outsourcing of the respondents. The ability to integrate real time data from multiple sources is an information management problem that many large companies struggle with. It is therefore perhaps not surprising that such a response profile has been generated by this question.

What is positive is that 26% of respondents were able to detect and identify an external attack. When further queried on the nature of the attack it is evident that the predominant attack was one against the respondent's internet or telecoms infrastructure. While the sample size is reduced to only those 26% of respondents that reported an incident, the Authors are reasonably confident that this is an accurate representation of the types of attack as the data is very similar to that reported in ISBS2012.

## If you answered 'yes' what was the nature of the incident?

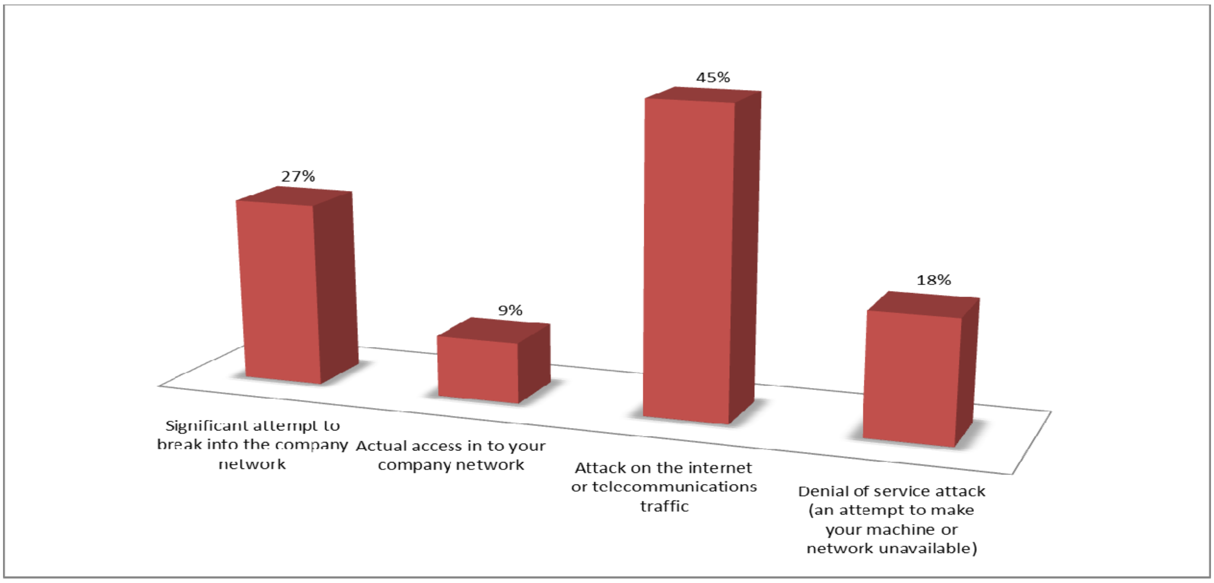

Figure 31 Nature of the Attack

### Worst Incident and Associated Costs

A crucial part of ascertaining the impact of any security incident is by understanding and quantifying the financial cost to the company experiencing the incident. It is only by gathering this information that an appropriate level of security investment can be justified. The final series of questions inquired as to the worst security incident the respondent had suffered and followed this up with an exploration on the costs that were incurred as a result of the incident.

Figure 32 provides a representation of the data and shows that the worst incident suffered by the respondents was system failure or data corruption (21%) followed by malware (17%).  This is in line with the profile of the incident responses shown previously in the document in Figure 25.  In addition to this 13% of respondents were unsure of what the worst incident was most severe which would appear to indicate an inability or lack of a process to measure this impact.

Following on from identifying the worst incident experienced by respondents they were then asked to consider the costs associated with recover, direct and indirect financial loss. The respondents were also asked their opinion on the impact to the company's reputation.  It should be noted that the data used to generate these results was only obtained from a small subset of the respondents and so cannot be statistically relied upon to be representative on a larger scale. The data given in Figure 33 to Figure 36 is provided purely for completeness.  However, given that the small data set size prevents any meaningful in-depth analysis, the Authors have drawn broad conclusions which are indicative of the data.

The first notable piece of data is the majority of 'unsure' responses. This clearly indicates that many respondents lack the capability to measure the impact of a security incident in clear financial terms. This therefore creates an information void preventing effective decision making in information security budget planning. There is a clear need for a simplistic approach to recording and evaluating incident impact for companies in the Micro and Small category in order to facilitate better decision making.

### In terms of security incident(s) you have experienced in the last year which was the most severe/disruptive to your company?

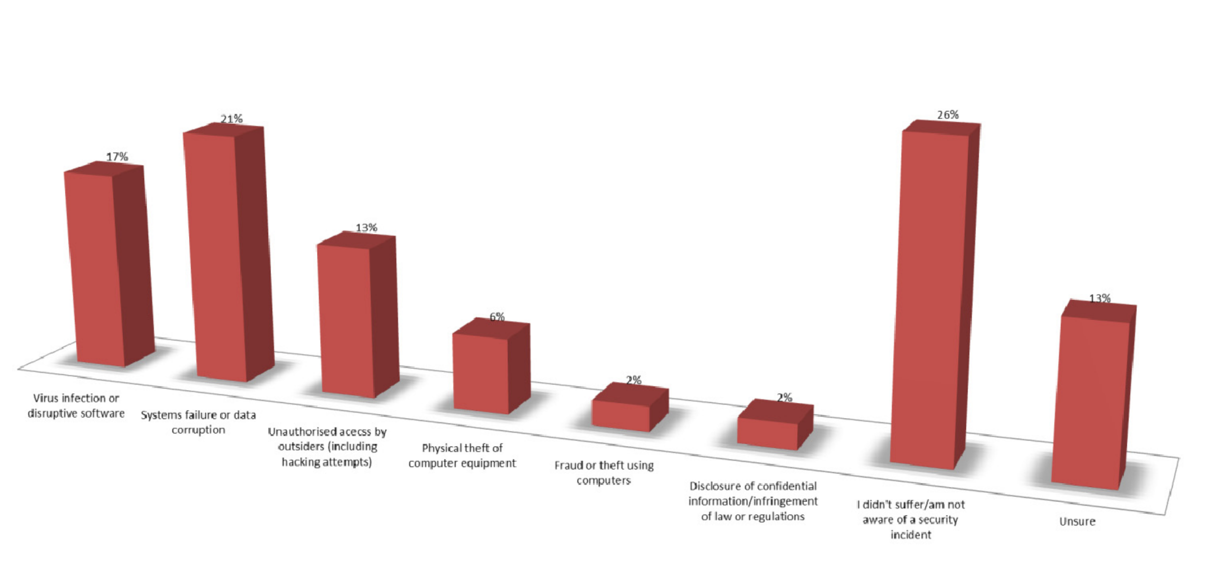

**Figure 32 Nature of the Worst Incident**

Another second notable observation is the number of respondents in the not applicable (N/A) category. One possible interpretation of these responses is that the respondents felt that the incident did not have a cost value attached to it in terms of recover and loses. However, this clearly cannot be the case as any remedial action must have direct costs in terms of people required to recover the situation, potential downtime of critical infrastructure and associated indirect cost of lost work capacity of affected staff.

This attitude perhaps reflects an assumption often found in small companies and start ups that employee time is essentially free. However, it is most likely that staff time is the most significant cost to the business certainly in terms of the associated opportunity cost. If nothing else, better cyber security provision could underpin a more productive work force in the same vein that Health and Safety controls prevent accidents and thus lost productivity.

A similar picture is seen when we look at reputation impact. Largely the companies report that there is limited reputational impact from the security events and that many of the event impacts are Non-Applicable (N/A). While this may be the case at the moment, trends in legislation are starting to place increasing requirements on companies to disclose incidents and breaches. If this information is to be required to be produced by law then this has the potential to have a significant impact on a business' reputation. Of greater concern is the link between any security incident and the impact on the data a company holds on their own customers. It is not clear from the data in this survey whether respondents understand that the majority of the worst incidents reported could have potentially disclosed confidential client information thus putting them in breach of their data protection responsibilities.

## In relation to the security incident from the previous question, how much cash expenditure was needed to recover from it?

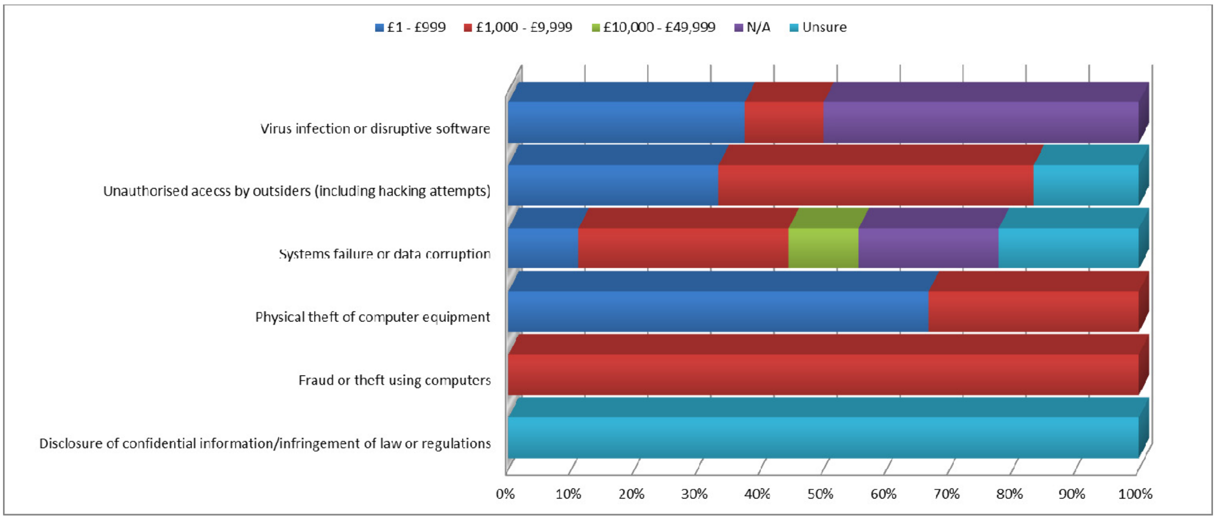

Figure 33 Cost in Relation to Recovery

## In relation to the same security incident, please estimate any direct financial loss associated with it

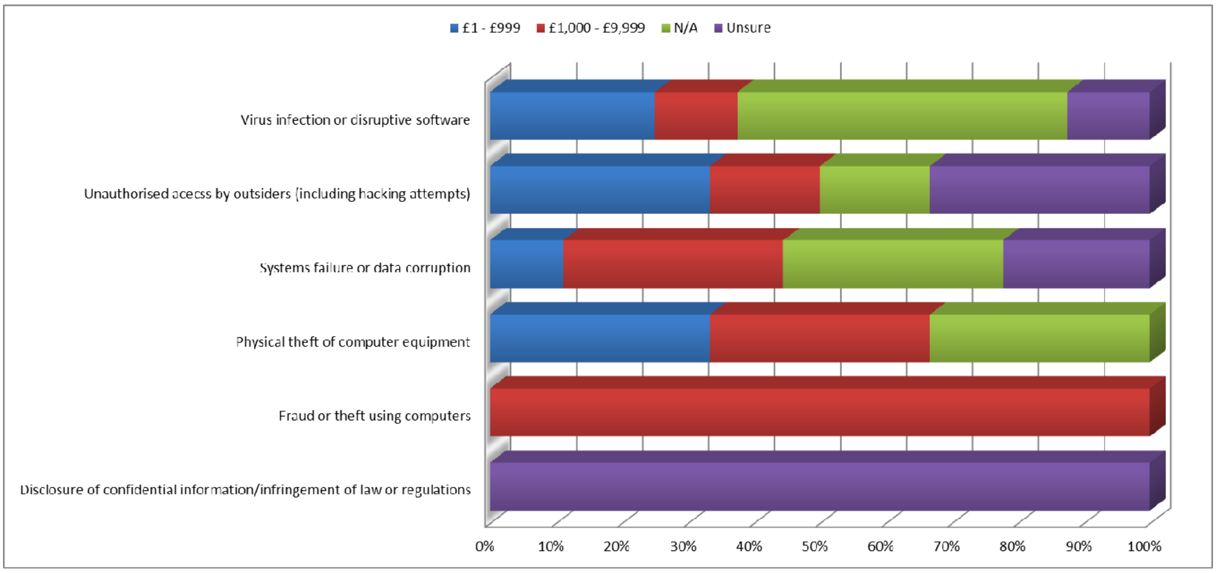

Figure 34 Direct Costs Incurred due to Worst Incident

## In relation to the same security incident, please estimate any indirect loss associated with it

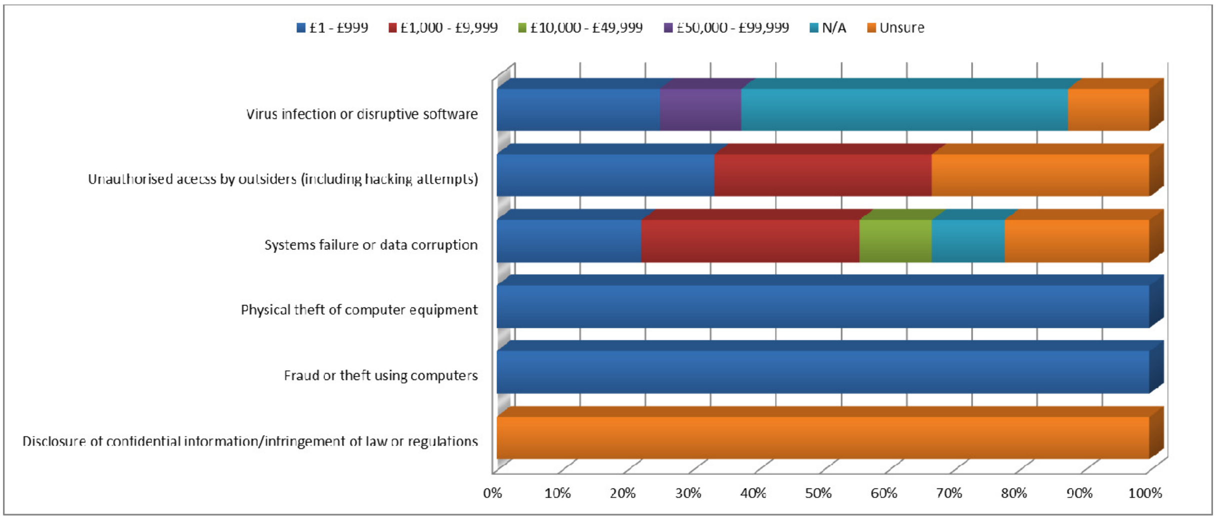

**Figure 35 Indirect Costs Incurred due to Worst Incident**

## In relation to the same security incident, to what extent do you feel the incident damaged the reputation of your organisation?

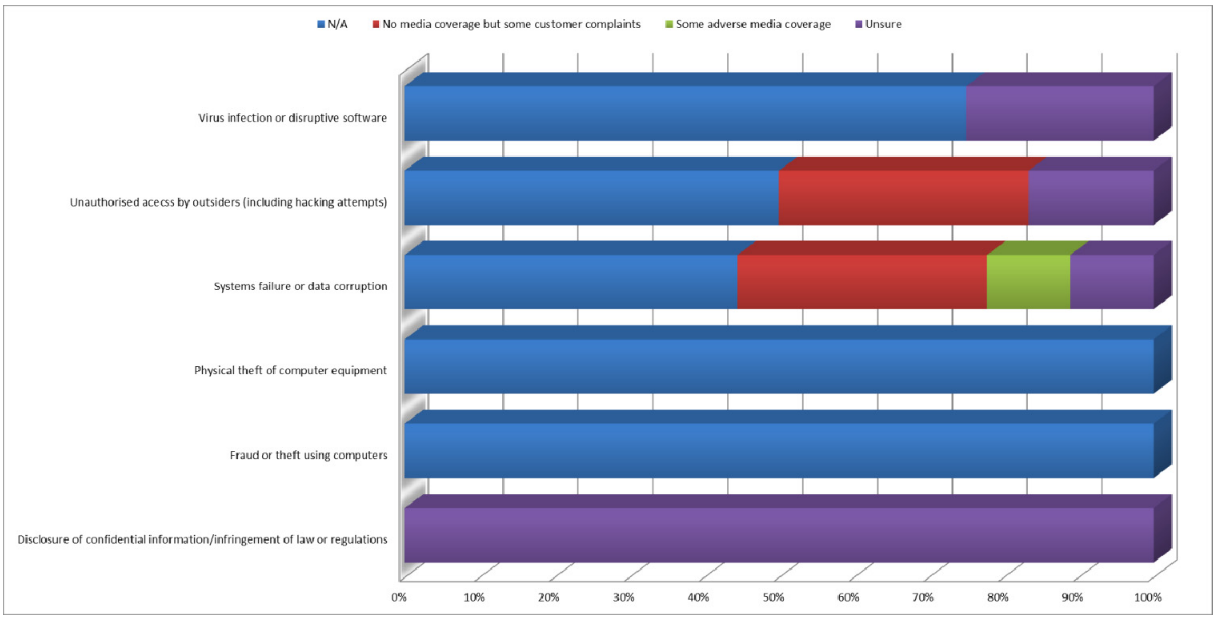

**Figure 36 Damage to Reputation due to Worst Incident**

## References

David Kennedy, 2012. *The Social Engineering Tookit.* [Online]
Available at: http://www.social-engineer.org/framework/Computer_Based_Social_Engineering_Tools:_Social_Engineer_Toolkit_(SET)
[Accessed October 2012].

Department for Business Innovation and Skills, 2011. *Business Population Estimates for the UK and REgions 2011,* s.l.: BIS.

European Commision, 2005. *The New SME Definition: User Guide and Model Declaration,* s.l.: Enterprise and industry publications.

Metasploit, 2012. *The Metasploit Framework.* [Online]
Available at: http://www.metasploit.com/
[Accessed October 2012].

PWC, 2010. *Internet Security Breach Survey 2010,* s.l.: PWC.

PWC, 2012. *Internet Security Breach Survey 2012,* s.l.: PWC.

Security Lancaster, 2012. *Cyber Security Conference 2012.* [Online]
Available at: http://www.security-centre.lancs.ac.uk/conferences/csc2012/
[Accessed October 2012].

Taleb, N. N., 2010. *The Black Swan: Second Edition: The Impact of the Highly Improbable: With a new section: "On Robustness and Fragility".* 2nd edition ed. s.l.:Random House Trade Paperbacks.

# Authors

### Dr Daniel Prince: Security Lancaster Associate Director for Partnerships

Dr Daniel Prince is an associate director and business partnerships manager for Security Lancaster. Prior to this he was the course director for the multi-disciplinary MSc in Cyber Security teaching penetration testing, digital forensics and information security risk management.

### Mr Nick King: Business Development Manager, School of Computing and Communications

Nick King is Business Development Manager in Lancaster University's School of Computing and Communications, located at InfoLab21. In addition to leading the Schools' Business Development Team Nick also Manages one of the Schools key Business Support Projects: ISTEP. Prior to his time at InfoLab21 Nick was UK Business Manager with a UK IT Solution Provider with a specialism in information assurance and security products/services.

**Science and Technology Business Partnerships and Enterprise**

Science and Technology | LANCASTER UNIVERSITY

As well as working with a range of external partners, ICT and Security form part of a wider theme based team across Science and Technology at Lancaster who offer expertise in:

- Advanced Manufacturing
- Energy
- Environment
- Health & Human Development
- Quantum Technologies
- Mathematics and Statistics

**Working in Partnership**

Across the themes we form collaborative partnerships around these 5 key areas:

- Collaborative Research and Consultancy
- Training and Education
- Co-location and Secondment
- Student Placements
- Product Development and IPR

***For more information regarding this report please see: http://www.security-centre.lancs.ac.uk/sbcss2012***