4.0 Results, Analysis and Discussions

4.1 Introduction

This chapter sets out the results of the questionnaire and provides supporting critical discussion of the respective results. Accordingly the chapter is sub-divided into a number of sections which correspond with the sections of the questionnaire as set out in the previous chapter. As this study has adopted a predominantly interpretive approach the only statistical analysis in this study is to provide descriptive statistics which help to identify preferences amongst the research population for certain types of information assets and security management. These then form a useful platform from which to launch the qualitative questions which help to explain the responses to the former sections.

4.2 Descriptive Statistics - Demographics

This section of the questionnaire sought to gather data on the demographics of the research population so as to understand factors such as the average age of the business, and size of the business under review in terms of turnover and number of employees, and also industry sector. The results are displayed in turn below:-

Age of the Company: The first questionnaire in the research instrument sought to establish the length of time a company had been in existence, as broadly speaking the older a business the more likely it is that they will have information assets of some kind that need to be secured. The results in table 4.1 below demonstrate that the greatest proportion of SME's had been in existence for between 5 and 10 years with 29% of the population indicating this was the case. Interestingly 24% of

respondents indicated that their business was between 1 and 3 years old which would coincide with people starting up a business after redundancy during the most recent recession. This also tallies with figures from the ONS (2011) who indicate that business start ups are at their highest levels for a number of years. The wider implications of this are that younger businesses with fewer resources are less likely to be aware of the need to protect their information assets unless the business owner in question already had some knowledge of this from previous employment experience.

Table 4.1: *Age of the Company*

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0 – 1 year	16	16.00	16.00	16.00
	1 – 3 years	24	24.00	24.00	40.00
	3 – 5 years	13	13.00	13.00	53.00
	5 – 10 years	29	29.00	29.00	82.00
	11+ years	18	18.00	18.00	100.0
	Total	100	100.0	100.0	

Size of Company by Turnover: Table 4.2 sets out the responses to the second question which sought to detail the size of the company by turnover. The results demonstrate that 95% of those companies surveyed have a turnover of less than £1 million which is broadly aligned with the data gathered by the ONS (2011). Interestingly the most popular response was for businesses in the range £250,001 - £500,000 which would suggest that the greatest proportion of businesses were well established as it is unlikely that a business which was very young (less than a year or two) would be able to generate that level of turnover. Further analysis demonstrates that 74% of all SME's surveyed had an annual turnover in excess of £100,000 which would imply at least some level of investment in software and

hardware of some variety, and also a number of information assets that would need to be protected.

Table 4.2: *Size of Company by Turnover*

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	£0 - £100,000	26	26.00	26.00	26.00
	£100,001 - £250,000	18	18.00	18.00	44.00
	£250,001 - £500,000	33	33.00	33.00	77.00
	£500,001 - £1,000,000	18	18.00	18.00	95.00
	£1,000,001+	5	5.00	5.00	100.0
	Total	100	100.0	100.0	

Size of Company by Number of Employees: The third question sought to establish the size of company by the number of employees. The reason for this that the data from the ONS (2011) would suggest that there is an increasing number of smaller companies which place greater emphasis on providing value and therefore have a smaller number of employees who generate a higher level of turnover with lower overheads. This is facilitated by factors such as internet marketing and virtual office facilities which help to keep costs low. The detail in table 4.3 below demonstrates that a greater proportion of SME's have between 11 and 25 employees (37%), followed by 23% of SME's which have between 26 and 50 employees. 19% of businesses are "micro" businesses with sub 10 employees under the BERR (2008) definition and only 4% of SME's have in excess of 100 employees. These results largely correlate with the findings for the preceding questions that a significant proportion of SME's are young and place a greater emphasis on intellectual capital as opposed to manufacturing or production.

Table 4.3: *Size of Company by Number of Employees*

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 – 10 employees	19	19.00	19.00	19.00
	11 – 25 employees	37	37.00	37.00	56.00
	26 – 50 employees	23	23.00	23.00	79.00
	51 – 100 employees	17	17.00	17.00	96.00
	101+ employees	4	4.00	4.00	100.0
	Total	100	100.0	100.0	

Industry Sector: The fourth question of the survey asked research participants to indicate the industry sector to which they most closely affiliated themselves. Unsurprisingly the two largest sectors were professional services such as business consultancy with 23%, and IT / IS services which included web design and systems development with 22% of the responses. These business sectors are typically characterised by high value revenue generation for low overhead because they rely heavily on intellectual assets and capital. It was surprising to see that 9% of respondents indicatd that they operated in the manufacturing sector which would probably suggest that they produced bespoke high value items for high margins. However, overall 85% of businesses surveyed would have a very strong reason to protect intellectual capital, and the remaining 15% (personal services) would doubtless have factors such as client databases and personnel records to consider.

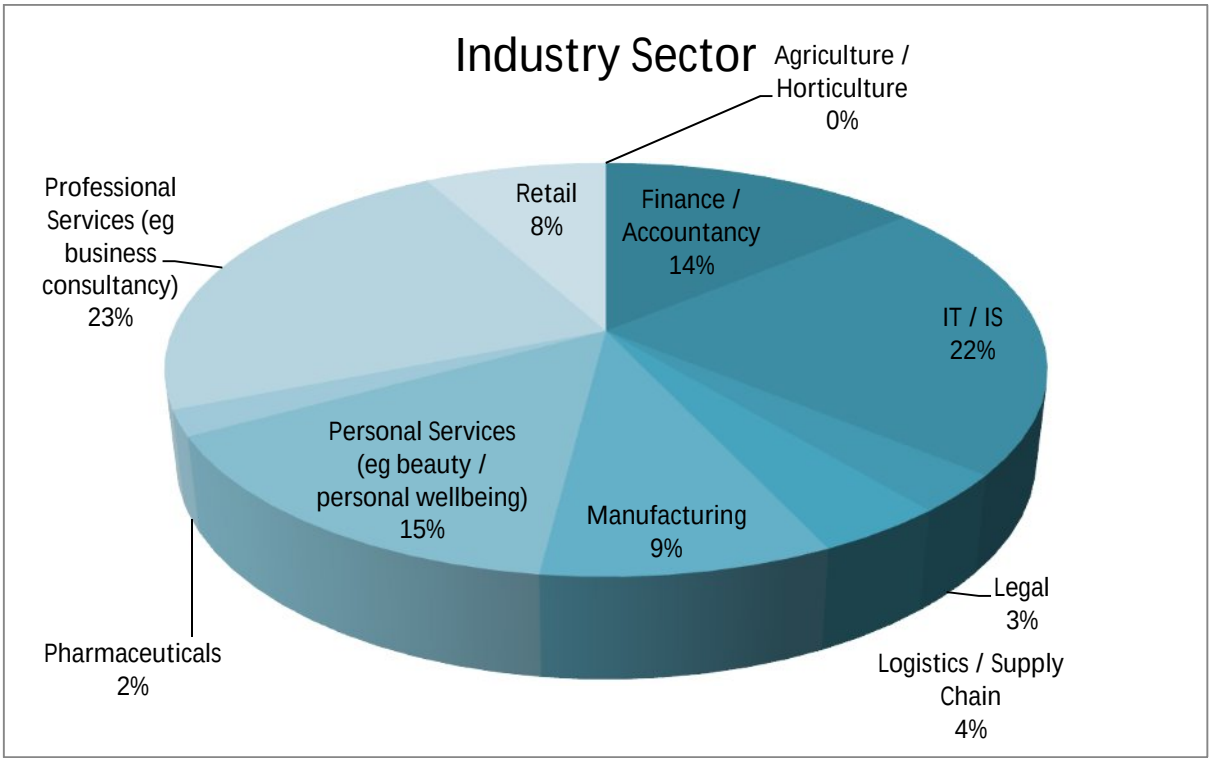

Figure 4: Proportion of SME's by Industry Sector

Protection of Information Assets: The final question in relation to the demographics of the research population asked participants to indicate whether they had any formal processes or procedures in place to protect their information assets. As the data in table 4.4 demonstrates, only 23% of respondents indicated that they had any formal means of protecting their information assets. This worrying statistic simply serves to confirm the data gathered in the literature review that very few SME's either appear to appreciate the critical importance of protecting information assets, or that they lack the resource (either financial or human capital) to address issues of information security and the protection of information assets.

Table 4.4: *Protection of Information Assets*

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	23	23.00	23.00	23.00
	No	77	77.00	77.00	100.0
	Total	100	100.0	100.0	

4.3 Descriptive Statistics – Perceptions of Information Assets and their Security

This section of the chapter sets out the responses to the statistical elements of the questionnaire. This includes the perceptions of information assets and associated security measures, the application of information security measures within an SME and also the known challenges of protecting information assets and applying recognised information security protocols.

4.3.1 Perceptions of Information Assets and Information Security

Perceptions of Information Assets and Information Security: Table 4.5 displays the results of the responses to the statements in respect of perceptions of information assets and security within SME's. As the results demonstrate very few SME's indicate that they have a clear understanding of some of the concepts surrounding information assets or their security. Recalling that the questionnaires were specifically distributed to employees at the SME's who have overall responsibility for information security and the protection of information assets (whatever their level of knowledge). The results would suggest that whilst a greater number of SME's feel comfortable with the concepts of information security and information assets in general, with mean scores of 3.38 and 3.22 respectively (which are above the statistical average), a worryingly small proportion are aware of concepts such as ISO 27001 and ISO 27002 and could explain them to a friend or colleague. This gap in understanding would provide the first indication as to why so few firms have adopted recognised information security protocols and thus fail to adequately protect their information assets. It is also concerning that for the

statement "*I make sure that I am aware of the latest developments in information security and that I pass these on to my colleagues*", only attracted a mean score of 2.15 suggesting that few SME's apply the necessary effort to understand the latest developments in information security which could be critical to protecting their business.

Table 4.5: *Perceptions of Information Assets and Information Security*

Statements	N	Mean	Std. Deviation
I have a clear understanding of the term "information assets" and could explain it to a friend or colleague	100	3.22	.702
I have a clear understanding of the concept "information security" and could explain it to a friend or colleague	100	3.38	.714
I would describe myself as having a high level of awareness as regards information security and its importance	100	3.31	.711
I make sure that I am aware of the latest developments in information security and that I pass these on to my colleagues	100	2.15	.619
I am aware of ISO 27001 and ISO 27002 and could explain them in suitable terms to a friend or colleague.	100	2.03	.591
Valid N	100		

4.3.2 Application of Information Asset Security within your Organisation

Application of Information Asset Security: The next element of the questionnaire sought to establish the extent to which those SME's who were surveyed protected their information assets and what methods they used to do so. The responses are displayed in table 4.6 below. Recalling the responses to the previous section it is unsurprising that the responses to the first statement of having "a robust attitude to information security" attracted such a low score of 1.22. This is attributed to a combination of having a reduced level of understanding as to the importance of

information security to protect information assets, a lack of resources and a lack of knowledge as to where to gather the necessary information from in terms of understating how best to protect information assets. The literature review revealed that many SME's find it difficult to gather information on best practice protocols for protecting their information assets and it is suggested that this is clearly displayed in these results. Thus it was also unsurprising that the highest mean score for this group of questions was in relation to the fact that most SME's perceived that they had a relatively weak attitude to information security and would probably not notice immediately if information assets were lost. However, despite the quite concerning responses in respect of the strength of actual information security procedures designed to protect information assets, it was clear that some effort has been made to protect information assets with many companies indicating that they had some form of process in place to protect information assets (3.16) and there was also evidence that SME's were trying to foster a culture of information security whereby employees had a heightened awareness of the value of their information assets and therefore took steps to protect and preserve them. This statement attracted a mean score of 2.83.

Table 4.6: *Application of Information Asset Security*

Statements	N	Mean	Std. Deviation
I would describe our firm as having a robust attitude to information assets and their security (we have full software protection, we constantly monitor the location of our information assets and we regularly review our procedures when situations change)	100	1.22	.402
I would describe our firm as having a moderate attitude to information assets and their security (for example we have anti-viral software and regularly check online activity)	100	2.68	.674
I would describe our firm as having a weak attitude to information assets and their security (we have little or no internet security, and would probably not notice immediately if we lost information assets)	100	3.41	.721
We have designed and implemented process controls to protect our information assets (such as encrypting data, regularly changing passwords, and backing up all company information on a regular basis)	100	3.16	.709
We recognise the value of our information assets and encourage employees to do the same by raising awareness and fostering a culture of security	100	2.83	.681
Valid N	100		

4.3.3 Challenges with Protecting Information Assets and Security Protocols

Challenges with Protecting Information Assets and Security Protocols: Table 4.7 displays the responses to the final quantitative element of the questionnaire which sought to understand attitudes towards known challenges of protecting information assets and the associated implementation of known information security protocols. As would be expected given the responses to the preceding two sections of the questionnaire, the responses to these statements clearly demonstrated that many SME's find the costs of protecting and monitoring their information assets using resources such as ISO 27001 and ISO 27002 were simply too much for a SME to bear. In consequence many SME's indicated that they did not apply these known protocols. It would seem that the greatest reason for not adopting ISO 27001 was

that it is regarded as being too rigid and inflexible for SME's as it received a mean score of 4.16. This is closely aligned with the findings of the literature review and anecdotally I was confirmed that many SME's felt that ISO 27001 was too restrictive for growing businesses which were constantly adapting to the challenges of their external environment. Although several SME representatives confirmed that they could see the benefits of ISO 27001 insofar as it would give wider stakeholders confidence in the business and the fact that they could protect information and ensure data security and integrity, they felt that ISO 27001 was simply too restrictive for their current operations and also in many cases too much of a regulatory burden. Other issues which were raised included that fact that for small, rapidly growing businesses the additional on-cost of perpetually retraining new employees and educating them as to the requirements of ISO 27001 was beyond their resources (4.03). Finally there was strong agreement with the fact that the requirements of ISO 27001 were incompatible with existing bespoke security systems (4.01).

Two overall issues can be noted from the responses to this section. Firstly, that the challenges with known information security measures were closely and strongly scored ranging from 4.01 to 4.16. This indicates that not only do SME's feel very strongly about the issues with ISO 27001 as a recognised approach, they also all seem to share the same issues with it. This perhaps highlights another significant issue with ISO 27001 overall in that it must strike a balance between rigidity and flexibility when seeking to secure information assets, especially where SME's are concerned.

Table 4.7: *Challenges with Protecting Information Assets and Security Protocols*

Statements	N	Mean	Std. Deviation
Our company finds it extremely costly and resource intensive to continually monitor and protect our information assets	100	3.22	.712
Although there are obvious benefits to ISO 27001 it is too costly to implement and maintain	100	4.08	.874
ISO 27001 is incompatible with existing security protocols we already have in our organisation	100	4.01	.861
ISO 27001 requires a very rigid approach to information security which is not appropriate for our business and resources	100	4.16	.889
The ongoing costs of training new employees to ISO 27001 standards is too much for a small business such as ours	100	4.03	.865
Valid N	100		

Having reviewed the quantitative aspects of the questionnaire, the following section analyses the themes which emerged from the qualitative aspects.

4.4 Qualitative Questions

The five qualitative questions were designed to assess the extent to which information security processes and metrics were used by SME's and what value they felt was delivered as a result. The themes from the five questions are shown below:-

1. *Do you have any other processes / procedures (outside of those mentioned above) that are concerned with information security? Please can you describe them?*

The response to this question ranged from quite detailed investment in IT and IS security procedures including reasonably sophisticated software checks for internet activity and email activity including scanning and encryption, through to very limited checks and in one or two cases virtually no security at all. Some SME's admitted

that because resources were so scarce they were happy to allow employees to share passwords and log into systems as one another for reasons of speed and efficacy. It is suggested that this is possibly the result of high levels of trust which are more evident in SME's and also possibly the fact that in smaller firms there is less knowledge of factors outside their core of expertise, so as a result they are less able to investigate issues such as IS security. Some of the firms surveyed indicated that they conducted random checks on IS security procedures but the vast majority indicated that they relied on trust to a large extent and rarely had the resource capability to perform large scale or sophisticated security checks. Furthermore, some respondents indicated that there was a lack of clarity of the term "information assets" and therefore it was unclear what should be secured and what should not be. The pragmatic reality of the situation seems to be in SME's it can in some ways be very difficult to implement any form of check and balance on information assets without breaching a difficult emotional barrier of trust (Williams, 2007). Furthermore, as a large proportion of SME's are family owned and managed the implementation of security checks would automatically imply a lack of trust which is likely to be highly damaging to employee morale.

2. *Have you any metrics or benchmarks to measure you internal information security processes? If yes, please can you explain them?*

The response to this question was largely negative as relatively few of the SME's surveyed indicated that they had any form of robust security process control and even fewer indicated that they had any form of metrics or benchmarks in place. Anecdotally it was observed that it was either IT / IS sector firms that had some form of process control metrics, and the larger of the SME's who had sufficient resource to devote to monitoring their information assets and their security. Some firms

indicated that they had adopted a “top-down” approach to information security metrics linking them to the overall objectives of the business. Other indicated that they had applied something more akin to a “six-sigma” approach where they sought to remove incremental bad practices such as a lax attitude towards passwords.

3. *If you have information security metrics do you find them to be useful / effective? Please can you explain why?*

Overall the firms who had engaged information security measures and metrics found that they had benefited as a result, but not necessarily in the manner in which they had envisaged. For example, firms who had adopted either a six-sigma approach to incremental bottom-up employee driven improvements found that overall the level of employee engagement had improved and the firm as a whole had seem benefits in other areas because there was more organisational cohesion. Firms that had employed a top-down down approach had found that the overall culture of the organisation had improved in regards to information security. For example, employees adopted stronger passwords and changed them more regularly, and they were also more cautious about what they emailed and where they emailed it to and from. Thus if an employee was working remotely they would take greater care of the security of the connection (wi-fi access in public areas being strongly discouraged). The overriding theme which emerged here was that employing information security approaches was worth the effort, although the results are not necessarily directly obvious.

4. *Have you ever tried to audit your information assets? If so please can you describe what happened?*

Of the 100 SME's surveyed, only 7 indicated that they had ever made any attempt to audit their information assets or perform any form of random check on their information security. These firms were all either in the IT/IS sector had in excess of 101 employees. In discussions it emerged that of these firms all of them had employed individuals who had specific prior experience of auditing information assets or information security which had been gained in much larger firms. This evidence provides a clue as to why many smaller firms are most probably not using such processes, *viz*, they have had no direct experience so they are ignorant of the fact that the adoption of such processes would be of benefit to their business in the long term. To some extent this echoes the literature which suggests that dissemination of the relevant information as regards information security is not forthcoming. When the firms were asked to describe the experience of auditing their assets, most indicated that the experience had in fact produced some fruitful results, especially in respect of how employees were spending their time when working remotely.

5. *As society moves toward becoming an information economy has your firm any future plans to update / implement information assets security procedures or processes in some form?*

When asked if there were any future plans to adopt information security / information assets management processes, approximately 40% of SME's responded positively insofar as they felt it would be of benefit to introduce some form of security process. However in discussions most indicated that they were unsure how best to design and implement a low or nil-cost culturally driven change. Once again, this tallies with the literature and previous results in that many SME's simply lack the necessary knowledge in areas outside their expertise. It would suggest that if the ISO and the

wider business community would like to improve information security, they would be well advised to consider how best to disseminate such valuable information so that more people were aware of the adverse effects of failing to protect their information assets. In the long term this would help to build growth in the wider economy.

4.5 Summary

This chapter has provided the primary results of the questionnaire with supporting analysis interpretation and discussion. It has been revealed from the results that very few SME's actively strive to secure their information assets which is both concerning and sadly not entirely surprising given the detail and information gathered in the literature review. The driving factors of this situation appear to be a lack of resource and a lack of understanding. Those firms who do actively seek to monitor and secure their information assets have found a number of quantifiable and non-quantifiable benefits have ensued including an improved organisational culture, improved organisational efficiency and also improved profitability (as a consequence of the preceding factors). Invariably firms that have applied information security metrics are larger firm with sufficient resource and knowledge or IT / IS centric firms who have exposure and experience. The following chapter will provide the overall conclusions of this study and a series of recommendations for SME's looking to improve their level of information asset security.