What Business Environment changes are needed to cause SMEs to take a strategic approach to Information Security?

Richard Henson,
Senior Lecturer in Computing,
Worcester Business School
Worcester UK
Tel +441905 855397

Dr Joy Garfield,
Senior Lecturer in Computing,
Worcester Business School
Worcester UK
Tel +441905 542368

1. Abstract

In the fourteen years since "Economics of Information Security" started as a discipline, many articles have been written about management of information security within organisations. Most of the articles have focused on public sector or larger private sector companies perhaps with an implicit assumption that the research findings would also apply to and influence SMEs. In practice, the truth is that SMEs have been largely unmoved, and not enough research has examined this reality.

In this paper, the author seeks to explore the reasons why smaller SMEs in particular have consistently failed to see securing information as strategic year-on-year spending, and often just part of an overall tight IT budget. Spending on security therefore has to compete with demands for hardware, infrastructure, and strategic applications.

The author's latest research scrutinises the typical SMEs reasoning choosing to see non-spending on security as an acceptable strategic risk. In terms of primary data-gathering, it looks particularly at possible reasons why SMEs tend not to take much notice of "scare stories" in the media which have consistently shown that SMEs are increasingly at risk as the information systems of larger businesses have taken greater precautions and become more difficult to penetrate.

The results and their analysis provide useful pointers towards the broader business environment changes that would cause SMEs to be more risk-averse and ethical in their approach to securing their own and their clients' information.

Keywords: SME, Information Risk Management, Information Assurance, ISMS, Information Security Management Systems, Data Protection Legislation, EU Data Breaches Legislation, Economics of Information Security, Supply Chain, ISO27001, PCI-DSS, Cyber Essentials,

IASME.

2. Introduction

In the early days of computing, information security management focussed on physical security and large companies. All automated processing happened in one area and that was kept secure. Even when computing transferred to dumb terminals in the late 1970s, the main issues were screening of staff and confidentiality of passwords. Most SMEs were paper-based, and only larger companies could justify the cost of computer hardware and software, and associated staff, which were all very expensive. However, through the 1980s the desktop PC progressively made it possible for small businesses to utilise small, cheap, and effective desktop and portable computers for a range of tasks, and portable storage devices became available, providing scope for data breaches (Brancheau & Wetherbe, 1987).

Securing information became an issue for organisations from the moment they started using desktop computers for creating and manipulating data, rather than centralised and physically secure server clusters with access to staff only via dumb terminals. The data could now be stored and processed on a local machine, and was beyond the control of data processing experts with knowledge of secure information handling. However, remarkably, the problem was not widely acknowledged by organisations (Brancheau & Brown, 1993).

By the 1990s, desktops and portables were networkable and could exchange data, and portable storage up to 700 Mb became available through CDs. For the first time, there was a danger of serious corporate data loss from the SME through digital devices. However, the information security focus remained on the larger companies who by now were using their large computers to communicate data worldwide using public networks. In the UK, SME security should have been scrutinised to ensure adherence the 1984 Data Protection Act (HMG, 1984), but in the absence of reported breaches continued to fall below the radar.

During the 1990s, localised CPU power increased immensely, portable storage up to 4 Gb became available, and even small computers could link up to public networks for exchanging data. The scope for data breaches became immense, and this didn't escape the eye of the concerned academic. The matter of company data being saved in an unsecure place only became a major issue for organisations once they started connecting their systems to the Internet, potentially exposing their personal and sensitive data. Once this practice became well known, they were easy prey for hackers. Although this danger had been anticipated by IT managers in the early days of "end-user computing", they continued to be largely ignored by senior managers who were attracted by greater convenience and reduced cost. Many "old school" IT managers were laid off in the early 1990s wave of restructuring, and the problem for smaller organisations became "out of sight". This was explored and discussed in an earlier article (Henson & Kuzma, 2010).

The concerns about large organisations and their data remained, and a British Standard for Information Security Management (BS7799) was introduced (BSI, 1998), at least partly because in this context security was often seen as a "product" not a process, and putting a

management system in place was clearly a sensible way forward. However, this was correctly perceived as time consuming and costly, so even large organisations avoided a process-based approach. However, by the early 21st century, thanks largely to Anderson (2001) and Schneier (2002) the new field of "Economics and Information Security" opened up. A new prestigious academic workshop, WEIS (Workshop on Economics of Information Security), started to meet annually, and many papers were presented and discussed to keep the corporate world informed of the latest technologies, and the latest risks, and the connected world became the hyper-connected world increasing the potential vulnerability to attack still further. BS7799 was more widely adopted and in 2005 became an International Standard, ISO27001 (ISO, 2005). However, as late as 2009, WEIS had received little input regarding the information security of SMEs. One of the authors of this paper remarked about this fact at the WEIS conference that year, quoting the University of Worcester research of the time (Arthur, 2009), and other private sector research (Ernst & Young, 2008) as evidence that most SMEs still weren't interested in information security. This research was consistent with government's own findings across the whole of the UK. But these were SMEs. Did this even matter?

This problem has been addressed in a number of ways in recent years, but the response from SME owners has consistently been underwhelming. As one academic working in this space commented… "There is a need, but not a want". This paper seeks to find some answers to the question "Why do many SMEs continue to show indifference to information security?" particularly with regard to taking action to establish information assurance within their own organisations. The results suggest that the problem is one of perception of information assurance, and this is now engrained in our small business culture. Whilst measures such as small-scale financial assistance and cyber liability insurance do have a small effect on perception and culture, a response is needed at a national level to bring about culture change.

Similar changes in perception happened between the 1960s and 1980s in terms of drinking and driving and wearing seat belts, but of course cultural changes take time. In the mid-1960s a UK law was passed saying they must be fitted on new cars, but no law was introduced saying people should wear them until the mid-1980s. This left a period of 20 years and an accumulation of unnecessary road deaths before a combination of data and public information films (e.g. "clunk-clink every trip") changed the public mind sufficiently for the legislation to be brought in without too much dissent.

There has been much discussion over a number of years about whether to, or not to, legislate to bring information security under greater control (Sinha & Gillies, 2011). In at least one of the authors' opinions, there is no point in legislating if a majority of the public does not see the need to do so. This may be analogous to the matter of seat belts in cars. The matter of educating a hostile British public to adopting the use of seat belts over a period of time shows that public opinion can be shifted in a strategic way, but it takes time – and planning.

3. Information Assurance Developments in the SME Space

Previous studies (Coles-Kemp & Overill, 2007; Barlette & Fomin, 2008) have shown that the ISO27001 Information Security Management standard, whilst becoming increasingly popular for larger companies, is very rarely contemplated by SMEs. Small companies would generally not have the expertise or understanding to appreciate the risk to their business as a result of not having secured their data. The reason most frequently quoted was cost, although time and complexity were also negative drivers. In other research, Fomin et al (2008) also identified a number of negative drivers on SMEs in their research on several European countries; the matter of positive and negative drivers for SMEs was enhanced and expanded by Henson & Hallas (2009).

Since 2009 much has happened to encourage SMEs to improve their information handling habits. The existing International Standard (ISO27001) was generally considered to be difficult for SMEs, and nothing any more suitable was commercially available (Henson & Booth, 2010). A new Information Assurance standard, IASME, was therefore developed with Technology Strategy Board funding (Henson et al, 2011), and there was a highly publicised acknowledgement in the US that the supply chain needed to be more secure and this needed to happen with the cooperation of SMEs (Wilson & Ali, 2011).

IASME was based on selecting and auditing a smaller number of controls, whilst providing a route to full ISO27001 certification. Later, a self-assessed, and therefore cheaper option for assessment against the IASME standard was devised, which aligned with the much simpler Cyber Essentials (BIS, 2014) which was solely based on self-assessment against five physical controls. The previous excuse by SMEs that it was too expensive to get IA certification looked less viable. Moreover, the updated 2013 version of the ISO27001 standard allowed much more flexible use of agreed sets of controls – so the 114 recommended as ISO27001 annex A are no longer mandatory (ISO, 2013). The updated International Standard also provides a focus on controls across the supply chain, which will be of particular interest to SMEs, if they could see the value of having an ISMS (Information Security Management System).

In addition to this a progressive improvement in options available to SMEs, the availability of Innovation Vouchers (BIS, 2013) to help with consultancy costs, and progressively increased penalties for being negligent with digital information, it might have been expected that SMEs would take heed and improve their focus on looking after their information assets. However, research on the ground showed that this is still generally not the case. Statistics consistently show that more small businesses are being breached every year. However, according to statistics from the three main awarding bodies (IASME, 2015; CREST, 2015; QGMS, 2015), the take up for Cyber Essentials so far has been good but not overwhelming, and interest in IA systems has not increased appreciably, in terms of the accredited companies opting for a more exhaustive audited CyberEssentials+ programme. Indeed the latest government statistics on SMEs (BIS, 2015) suggested that despite projected overall growth, SMEs intended to spend less on protecting data in 2015 than they spent in 2014, despite the availability of Cyber Essentials from June 2014. Worldwide research (Ponemon, 2015) shows

similar statistics in other countries, although the authors have not investigated the sweeteners available in those countries.

The question remains, therefore, “Why not?” Looking at the UK, why are smaller businesses so reluctant to take the steps necessary to secure that precious data that enables their organisation to do business? One previously-explored hypothesis that is “market failure” (Henson & Sutcliffe, 2013), with a potential solution to alter SME perception being provided by cyber liability insurance. However, the UK cyber insurance market still doesn’t seem to be too much greater than negligible, and the authors thought it might be useful to ask small business owners some questions about information security that might provide insight into the nature of the problem and how it can be overcome.

Cyber insurance has certainly worked to raise awareness and protect the supply chain in the US (Garrie & Mann, 2014). However, the US is one country that has raised SME awareness to the point of taking information security seriously enough to insure against data breaches. It appears that the main driver for cyber insurance is the fear of litigation, most likely as a consequence of quite stringent regulation about the reporting of data breaches. This spread rapidly, state-by-state, starting with California in 2003 (State of California, 2003).

Surprisingly, similar legislation didn’t occur elsewhere. However, belatedly, a similar law was discussed over several years (Ashford, 2013) was finally agreed, and is to be implemented across Europe from the start of 2016 (EU, 2014; Computer Weekly, 2015). This very existence of further legislation may bring about a change in attitudes. However, the UK is currently debating whether or not to pull out of Europe so the introduction of this EU-based legislation may not be as much of a positive driver for UK SMEs to invest in protecting their data as some may think. In the short term, the impending UK referendum vote () will probably focus the minds of UK citizens in preference to adhering to an EU Regulation that they may not have to abide by anyway. It is unlikely that the matter of perception change, and consequent attitude change to the reality of data breaches will probably have to wait until after the referendum has passed. So how bad is the perception problem, and can the UK afford to wait until 2017?

The purpose of this study is to prove/disprove whether it is true that SMEs do still have a negative attitude to most things cyber, and to drill down into attitudes based on identified categories to see how entrenched they are, and to help inform any future campaign to influence SME perceptions, when it finally gets the go ahead on a national scale.

4. Hypothesis

SMEs have negative attitudes towards information security generally. This explains a perceived reluctance spend in this area (Henson & Hallas, 2009), and represents a powerful driver against putting more resources into information security. However, dividing attitudes into four categories, the question can be subdivided for greater granularity:

H1: SMEs have a negative attitude towards Information Assurance

H2: SMEs have a negative attitude towards Data Breaches and the Law

H3: SMEs have a negative attitude towards Spending on Cyber Security

H4: SMEs have a negative attitude towards Business Risk.

5. Methodology

The research was conducted online, using a SurveyMonkey online questionnaire, using a similar technique to that applied by Arthur (2009) for a previous SME survey, and using lessons learned from the survey to ensure that the person completing the questionnaire is the owner or a senior manager and not an IT manager (as may otherwise be the case for a questionnaire involving IT matters).

The hypotheses will be tested through a set of 28 online questions, divided into the four above categories. The questions for each category will attempt to establish some reasons why SMEs consistently refuse to engage with attempts to encourage them to use a systematic set of controls or develop an ISMS.

Through the data supplied by SMEs, this research seeks to improve understanding of how the apparently complacent SME cyber security mindset has arisen and postulate possible strategies for changing it. A more rational view of this ever-increasing problem is essential for a number of reasons, not least that the new EU data protection legislation will be taken very seriously by UK SMEs. Of course, it is also reasonable to say that SMEs will only take the new legislation seriously if they think it is being policed, and as this is a civil law, responsibility currently lies with the ICO (Information Commissioners Office).

6. Implementation of Methodology

The URL of this online questionnaire with mostly closed questions was distributed to a random selection of SMEs via email. The SME respondent had to give a response between 1 and 5 according to a Lickert scale for each of the 28 questions. Some general questions such as business size and sector were also asked. The incentive for completing the questionnaire was two half-days free consultancy towards Cyber Essentials (CE) or CE-plus.

Care was taken to ensure that the survey went to the email address of the head of the organisation or a senior manager. Previous surveys on SMEs and aspects of information security have often been erroneously passed on to the IT manager for completion, and this study would be invalidated if not completed by a senior member of staff. The email lists used were from the SME contacts of two universities, one in the West Midlands and the other in South Wales, and they are both random samples of SMEs covering all sizes and sectors.

6.1 Results (see appendix 1)

6.2 Treatment of Results

Survey Monkey captures the raw data, and then provides statistical data for each individual response, on an Excel spreadsheet. The questionnaire had been designed so that some of the responses showed 1 as a positive attitude, whilst others showed 5 as positive. This was to ensure that the respondent didn't try to guess a "right answer" based on a pattern. The spreadsheet was kept confidential, although no SME names were required to complete the questionnaire.

Overall data covering all of the individual 28 questions had to be "standardised" by taking account of whether a score of 5 or 1 showed the negative attitude. Once individual questions had been appropriately corrected, aggregated, and presented, similarly meaningful data could be provided for each category.

The following questions were designed with "1" showing a negative attitude:

- Information Assurance standards are unnecessary for the small business +0.08
- I'd like my business to conform to an information assurance standard but the costs are much too high -0.87
- Small businesses don't need to spend much money on cyber security because they have little information that would be useful to a hacker +0.86
- I'd be prepared to pay a little for information assurance, but I cannot afford to allocate time and someone would have to do it for me -0.71
- I'd be interested in Cyber Essentials if a self-certification route is possible and the certification cost is very low -1.33
- ISO27001 is only useful for very large businesses +0.07
- Cyber Essentials or any Information Assurance scheme has a use only to the larger businesses with fifty or more employees +0.29
- Small businesses are unlikely to be hacked +0.71
- Breaching the data protection act is a civil not criminal matter +0.36
- If my business was hacked, I'd get it fixed and keep quiet about it 0
- I don't know of any small businesses that have been hacked and lost customers as a result -0.14
- If a business does get hacked they will very quickly know about it +0.29
- The Data Protection Act doesn't apply to charities or very small businesses +1.21
- Customers are more interested in price than protection of their personal data -0.43
- Small businesses need to concentrate on business objectives, and cyber security is an optional extra +0.5
- The reputation of a small business is unlikely to be affected if they are hacked +0.67
- Most of the cost of getting certified to an information assurance standard is peoples' time that could be spent on other business matters -0.17
- My business can be insured against loss of data without having information security safeguards in place +0.75

- My employees know about information handling and the potential threats to information systems through them -1.08
- Information risk assessment doesn't really apply to my business +0.83

Actual scores were subtracted from 3 and sign reversed to get the Standardised scores

The following had "5" as showing a negative attitude

- The small business should consider quality assurance standards as an important factor in choosing an Internet Service Provider (ISP) +0.93
- Information assurance is just another way for those ruthless security people to get money out of the small business +0.40
- I would be interested in using the government money available to small businesses wishing to gain an information assurance qualification like Cyber Essentials or IASME -1.33
- The law on data protection needs to be stricter +0.29
- Small businesses are unlikely to have a data breach through their business partners -0.53
- Not having information assurance of some kind might hinder future bids for contracts +0.85
- In future, the government won't enter a business contract with anyone unless they show some evidence of looking after data +1.5
- My reputation will be damaged if I suffer from a data breach and word gets out +0.83
- I could be put out of business if I don't protect my information systems +1.0

Actual Scores were subtracted from 3, and sign reversed, to get the standardised scores

Several questions were supplying information not attitudes. They supply useful information, which don't directly relate to any of the hypotheses:

- How many employees?
- What sector?
- How do you manage your data?
- "I'd not previously heard of IASME, Information Assurance for SMEs, before starting this questionnaire"
- "I'd not previously heard of Cyber Essentials, the government's new Information Assurance scheme, before starting this questionnaire"

6.3 Expected Results

The raw results would have to be "normalised, as described in paragraph 6.2. In order for any of the four hypotheses to be supported, the normalised scores for that category would probably need to have an averaged value somewhere between 0 and -2. Whether or not this was the case is shown in the next section.

6.4 Analysed Raw Data

Per question: (see appendix 1 for more detail)

Quite a differentiated overall picture. Highly negative on questions relating to Cyber Essentials and IASME (-1.5, -1.33) but highly positive about the need to protect the government supply chain (1.33) even though a major part of the raison d'etre of each of these was to protect the supply chain.

Overall, more questions showing a positive attitude (17 in positive territory, 9 showing negative scores).

Per category: (see appendix 2)

Great differences here… the hypothesis supported regarding the Information Assurance category, but aggregated score close to 0 for Spending on Cyber Security. The two other hypotheses were disproved quite comprehensively (both showing positive scores).

Comment [A1]: Could be merged together into a paragraph with a few more sentences explanation.

Whilst not all areas of information security were covered through the questions, Information Assurance seems to be the one that evoked a negative response from the businesses, and it is interesting that the question about quality that didn't actually specify that term scored positively with respondents, indicating a lack of understanding about information assurance and what it can do for them (and the supply chain).

6.5 Other data collected

In the course of contacting SMEs and collecting data, a number of anecdotes were relayed from concerned small businesses. Most cover issues that have been discussed in other papers and were discussed earlier in this article. One interesting addition, however, is the role of the professional organisation representing UK small businesses, the FSB (Federation for Small Business), at a local level, in apparently perpetuating the myth that SMEs, generally, are not at risk as long as they have up-to-date antivirus and a firewall.

This is very old advice. Yet the FSB website (FSB, 2014) provides online advice to its members that is much more rigorous, and much more appropriate for an organisation selling itself via its website or participating in online trading. From the excellent advice page, there has clearly been liaison with the government department responsible for the small business (i.e. BIS). Cyber Essentials was also produced by BIS in 2014 as the bare minimum. In addition to firewalls and antivirus, it also requires a patching policy, a user access policy and ability to configure devices as well as those two items. The evidence of this survey suggested that many SMEs still haven't heard of Cyber Essentials. It is a matter of some concern that large organisations can work together at a high level and come to an agreement, but that

agreement does not filter down to the fee-paying members. This will be discussed further in the conclusions of this paper and will be the subject of further research.

6.6 Discussion of “normalised” results

The data for all questions, averaged out, shows an overall response > 0. This confirms an overall positive response to cyber security by the small business.

However, when categories are investigated individually, there is clearly a negative response to Information Assurance, which is worthy of further investigation.

7. Conclusions

So, from scrutiny and analysis the data collected, the hypothesis that SMEs have a negative attitude towards information security is only partly supported. Moreover, the particular area that seems to be a negative driver against spending more has been identified.

Whilst this negative attitude to information assurance remains, SMEs are unlikely to be seeking to manage their information security according to established principles, let alone rushing to get certified against industry agreed standards, because they, remarkably, view information assurance with suspicion. It seems that one thing that is needed is a campaign to improve the standing of “cyber security experts” with SME owners. As discussed in a previous paper (Henson & Sutcliffe, 2013), this can be achieved either directly (e.g. government promotion) or indirectly (encouragement of cyber liability insurance, but only issuable if the organisation can show evidence of taking information security seriously). Low uptake of cyber liability insurance to date in the UK, in contrast to the rapid growth in the US (Garrie & Mann, 2013) suggests that costs and benefits to the SME have still not been correctly assessed to create a flourishing market.

It may well be the case that a few more years will need to pass before SMEs are ready to accept that they must take information security seriously and invest appropriately in it. This is very unfortunate. It is perhaps surprising that when the EU tightened up on data protection with a new directive in 1995 (EU, 1995) the UK had an opportunity to tighten its Data Protection legislation (HMG, 1998), but in effect the main change was to gradually (over the next seven years) bring paper-based data within the legislation. The US data breaches legislation in fact came into play before organisations in the UK were required to comply fully with 1998 Data protection Legislation!

Even now, those ad hoc Interviews with FSB members has revealed that, despite the best efforts of FSB and BIS leadership (FSB, 2013) the prevailing attitude is being supported, if not encouraged, by local representatives of one of the main professional organisations for small businesses. The advice adopted by other professional organisations for small businesses, such as the Chambers of Commerce, have not yet been investigated, but this also needs to happen. Also, the pressure that will be brought to bear on SMEs doing online trading

via the latest iteration of the online banking information assurance system (PCI-DSS) has yet to be investigated. This will be the subject of follow-up research.

Also, and perhaps partly because of a perceived business environment where SME systems are rarely successfully compromised, SME cyber-crime rarely gets reported. Even when reported, the detection rate is low, and this further encourages the cyber-criminal. Apart from this, statistics suggest that a huge amount of cyber fraud is happening in the UK, amounting to some £27 billion (Detica, 2011). This is not a satisfactory situation either for the businesses or the government aspirations of the UK as "a safe place to do business". It is also not good to have a criminal law in place (HMG, 1990; HMG, 2006) that is not being upheld due to a lack of the required police resources required to gather appropriate evidence to obtain a conviction (Yar, 2013).

One thing seems to be certain - if all these issues are not addressed, SMEs will continue to adopt a "head in the sand" approach and more and more will get their data breached or (worse scenario) taken out of the business. The perceived (negligible) and actual (considerable) instances of data breaches in SMEs can only be changed by businesses not staying quiet about being hacked and becoming noisy victims. For them to do this, a business environment needs to be nurtured that will encourage victims of SME cyber-crime to come forward.

So how can this change in perception occur? Advice given at local level is important, and that does need to be up-to-date. However, a lot rests with the printed, broadcast and online media, because of their role in shaping public opinion. Without labouring the point, which is a research paper in itself, broadcast media rarely report on data breaches, except through their websites. Whilst the public don't see cyber crime and cyber security as a high priority, police and other resources will continue to be directed on other matters, and local FSB reps will continue to play it down. The absence of a public perception in the UK that (a) cyber crime is increasingly hitting small businesses and (b) this really matters may be comforting, but it does not mesh with reality. We will ultimately come to a point where on-line business will be seen as too risky in the UK, compared to other countries (e.g. US, Canada, some EU members) that adopt a more mature attitude to reporting on and tackling these inevitable consequences of the information age.

To end on an optimistic note, the reverse, is of course also true. With careful guidance the UK could become a world leader in tackling cyber crime and combatting organisational data breaches, with the result that companies flock to the UK, as the safe place to engage in online activity and do e-commerce. The new EU regulation will apply to all European states, and there will be a form of "internal competition" among enlightened members to become Europe's safest place to do e-commerce. Wise EU states will be in competition to have the best record on SME cyber security and tackling cybercrime.

8. References

Anderson R, 2001, “Why information security is hard - an economic perspective” Computer Security Applications Conference, 2001, Proceedings, 10-14 Dec. 2001, Page(s): 358 – 365.

Arthur J, 2009, “Information Security survey of SMEs for Worcester Business School”.

Ashford W, 2013, "Proposed EU data breach laws will require proactive security", Computer Weekly [online at http://www.computerweekly.com/news/2240176411/Proposed-EU-data-breach-laws-will-require-proactive-security]

Ashford W, 2015, “EU Data Protection Regulation to be finalised by end of 2015”, Computer Weekly [online at http://www.computerweekly.com/news/4500248164/EU-Data-Protection-Regulation-to-be-finalised-by-end-of-2015]

Barlette Y & Fomin V V, 2008, “Exploring the suitability of IS security management standards for SMEs”, paper presented at the 41st Hawaii International Conference on System Sciences, Hawaii.

BIS, 2013, “Innovation Vouchers”, [online at https://vouchers.innovateuk.org/]

BIS, 2014, “Cyber Essentials: an overview”, https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

BIS, 2015, “Small Businesses Survey, 2014: Additional Analysis Data” [online at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/435820/Small_Business_Survey_2014_-__all_businesses_data.csv/preview]

British Standards Institution (BSI), 1998, “BS 7799-2:1998 Information security management. Specification for information security management systems”

Coles-Kemp L & Overill R, 2007, “The Design of Information Security Management Systems for Small-to-Medium Size Enterprises”

CREST, 2015, “Cyber Essentials Certified Companies”, [online at http://www.cyberessentials.org/list/]

Ernst & Young, 2008, “Global Information Security Survey 2008”, [online at http://www.ey.com/Global/assets.nsf/UK/Global_Information_Security_Survey_2008/$file/EY_Global_Information_Security_Survey_2008.pdf]

EU, 2005, “SME definition: User guide and model declaration” [online at http://ec.europa.eu/enterprise/enterprise_policy/sme_definition/sme_user_guide.pdf]

EU, 1995, “Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities, 1995”

EU, 2014, “Strengthening personal data protection”, [online at http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:52012PC0010]

Fomin V V, de Vries H, & Barlette Y, 2008, “ISO/IEC 27001 Information Systems Security Management Standard: Exploring the Reasons for Low Adoption”, EUROMOT 2008 Conference, Nice, France.

FSB, 2013, “Cyber security and fraud: The impact on small businesses”, [online at http://www.fsb.org.uk/frontpage/assets/fsb_cyber_security_and%20_fraud_paper_2013.pdf]

Henson, R & Hallas, B. (2009) "SMEs, Information Risk Management, and ROI". In: Athens Institute for Education and Research (ATINER) SMEs Conference 2009, 10th - 13th August 2009, Athens, Greece. (Submitted)

Henson, R & Kuzma, J (2010) End User Computing and Information Security: a Retrospective Look at the De-centralisation of Data Processing and Emerging Organisational Information Risk. In: UK Academy for Information Systems, 15th Annual Conference, 23-24 March 2010, University of Oxford
Henson, R & Sutcliffe, D (2013) A Model for Proactively Insuring SMEs in the Supply Chain Against Cyber Risk, Atiner Conference Paper Series No: SME2013-0547. ISSN 2241-2891
Henson, R, Dresner, D & Booth, D (2011) IASME: Information Security Management Evolution for SMEs. In: ATINER 8th Annual International Conference on Small & Medium Sized Enterprises: Management - Marketing, 1st - 4th August 2011, Athens
HMG, 1984, "Data Protection Act (1984)", Her Majesty's Stationary Office.
HMG, 1998, "Data Protection Act (1998)", Her Majesty's Stationary Office.
IASME, 2015, "Certified Organisations", [online at https://www.iasme.co.uk/index.php/companies-certified]
ISO, (2005), ISO/IEC 27001:2005, International Standards Organisation.
Ponemon Institute, 2015, "2014 Annual Study: UK Cost of a Data Breach", PGP Corporation.
QGMS, 2015, "Cyber Essentials Certified Companies", [online at http://www.qgstandards.co.uk/cyber-essentials-accredited-companies/]
Schneier, B, 2002, "No we don't spend enough", WEIS2002, [online at] http://www2.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/18.doc
Sinha & Gillies A, 2011, "Improving the quality of information security management systems with ISO27000", The TQM Journal, Vol. 23 Issue 4, pp.367 – 376
State of California, 2003, "California Database Breach Act", [online at http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020212_introduced.pdf]
Wilson & Ali, 2011, "The Biggest Threat to the U.S. Digital Infrastructure: The Cyber Security Workforce Supply Chain"
Yar M, 2013, "Cybercrime and Society, 2nd Edition" pp. 15-19.

Appendix 1: Category Results

Information Assurance

Information Assurance standards are unnecessary for the small business

The small business should consider quality assurance standards as an important factor in choosing an Internet Service Provider (ISP)

Information assurance is just another way for those ruthless security people to get money out of the small business

I'd like my business to conform to an information assurance standard but the costs are much too high

Positives: 1 (+1.08 total)

Negatives: 3 (-1.54 total)

Favours hypothesis!

Spending on Information Security

Small businesses don't need to spend much money on cyber security because they have little information that would be useful to a hacker

I'd be prepared to pay a little for information assurance, but I cannot afford to allocate time and someone would have to do it for me

I'd be interested in Cyber Essentials if a self-certification route is possible and the certification cost is very low

I would be interested in using the government money available to small businesses wishing to gain an information assurance qualification like Cyber Essentials or IASME

ISO27001 is only useful for very large businesses

Cyber Essentials or any Information Assurance scheme has a use only to the larger businesses with fifty or more employees

3 positive (+3.0)

3 negative (-3.12)

3/3 Very slightly positive. Hypothesis not supported

The Law and Data Breaches

Small businesses are unlikely to be hacked

Breaching the data protection act is a civil not criminal matter

If my business was hacked, I'd get it fixed and keep quiet about it

The law on data protection needs to be stricter

Small businesses are unlikely to have a data breach through their business partners

I don't know of any small businesses that have been hacked and lost customers as a result

If a business does get hacked they will very quickly know about it

The Data Protection Act doesn't apply to charities or very small businesses

Customers are more interested in price than protection of their personal data

Overwhelmingly positive. Hypothesis disproved (7 pos, 2 neg)

Risk

Small businesses need to concentrate on business objectives, and cyber security is an optional extra

The reputation of a small business is unlikely to be affected if they are hacked.

Most of the cost of getting certified to an information assurance standard is peoples' time that could be spent on other business matters

Not having information assurance of some kind might hinder future bids for contracts

In future, the government won't enter a business contract with anyone unless they show some evidence of looking after data

My business can be insured against loss of data without having information security safeguards in place

My reputation will be damaged if I suffer from a data breach and word gets out

I could be put out of business if I don't protect my information systems

My employees know about information handling and the potential threats to information systems through them

Information risk assessment doesn't really apply to my business **Hypothesis overwhelmingly disproved 8 pos /1 neg**