Athens Institute for Education and Research
ATINER

ATINER's Conference Paper Series
SME2016-2278

SMEs Attitudes to "Information Assurance" and Consequences for the Digital Single Market

Richard Henson
Senior Lecturer in Computing
Worcester Business School
Worcester UK

Joy Garfield
Senior Lecturer in Computing
Worcester Business School
Worcester UK

An Introduction to ATINER's Conference Paper Series

ATINER started to publish this conference papers series in 2012. It includes only the papers submitted for publication after they were presented at one of the conferences organized by our Institute every year. This paper has been peer reviewed by at least two academic members of ATINER.

Dr. Gregory T. Papanikos
President
Athens Institute for Education and Research

This paper should be cited as follows:

Richard Henson, R. and Garfield, J., (2017). **"SMEs Attitudes to "Information Assurance" and Consequences for the Digital Single Market"** Athens: ATINER'S Conference Paper Series, No: **SME2016-2278.**

Athens Institute for Education and Research
8 Valaoritou Street, Kolonaki, 10671 Athens, Greece
Tel: + 30 210 3634210 Fax: + 30 210 3634209 Email: info@atiner.gr URL: www.atiner.gr
URL Conference Papers Series: www.atiner.gr/papers.htm

ISSN: 2241-2891
5/10/2017

SMEs Attitudes to "Information Assurance" and Consequences for the Digital Single Market

Richard Henson
Joy Garfield

Abstract

It is now generally accepted that cyber crime represents a big threat to organisations, and that they need to take appropriate action to protect their valuable information assets. However, current research shows that, although small businesses understand that they are potentially vulnerable, many are still not taking sufficient action to counteract the threat.

Last year, the authors sought, through a more generalised but categorised attitudinal study, to explore the reasons why smaller SMEs in particular were reluctant to engage with accepted principles for protecting their data. The results showed that SMEs understood many of the issues. They were prepared to spend more but were particularly suspicious about spending on information assurance.

The authors' current research again focuses on SME attitudes but this time the survey asks only questions directly relating to information assurance and the standards available, in an attempt to try to understand exactly what is causing them to shy away from getting the badge or certificate that would demonstrate to customers and business partners that they take cyber security seriously.

As with last year's study, the results and analysis provide useful pointers towards the broader business environment changes that might cause SMEs to be more interested in working towards an appropriate cyber security standard.

Keywords: SME, Information Assurance, standards, cyber crime, Digital Single Market, GDPR, cyber security, attitudes, cyber liability insurance, compliance, certification, PCI-DSS, Cyber Essentials, IASME, ISO27001

Introduction

Whilst Cyber Security – or its non-identical predecessor Information Security – have been the source of much academic activity covering corporate and governmental IT over many years, the matter of SME cyber security was (sadly) not treated as a matter of major importance, either in the UK or in other parts of the world. There has, however, been considerable progress in recent years, and a number smaller businesses now engage actively with the increasing threats to their livelihoods posed by cyber crime. Also, regulations to be introduced in countries within the EU (EU, 2016) intend to establish a digital single market, with more stringent regulations to protect personal data used within that framework.

Many earlier papers have referred obliquely to positive outcomes for SMEs as a result of participating in cyber security enhancing activities (Goucher, 2011; Henson & Hallas 2009), but few have asked the SME what they want (or don't want!). Our own recent research has shown that many SMEs do now understand the arguments for improved cyber security, not just in terms of spending more, but also as regards keeping on the right side of the law and potentially getting new contracts and increasing market share. However, despite government and other efforts to introduce Information Assurance tailored that research suggested also that SMEs have a negative reaction to "Information Assurance".

This paper will examine SME attitudes to transforming business interest in security into auditable business activities that will provide good, systematic security practices in SMEs and other smaller organisations. The intention is to use SME responses to drill down into the detail of current SME perceptions on information assurance. This may help establish why the negative reaction to the term "information assurance" was evoked, and suggest possible ways to address this current obstacle and bring about better cyber security in organisations.

Background to Information Assurance

Information used by large businesses has been digitised since the 1970s (Dordick et al, 1979), and large organisations are generally well structured to deal with digital information efficiently. Our preceding article on SME attitudes (Henson & Garfield, 2015) looked historically at the development of digital information systems in small businesses, how they lacked expertise and remained paper-based for longer, how they fell behind "normal" organisational practice in the 1980s, and how they did not fully embrace the implications of the 1984 and 1998 Data Protection Acts (HMG, 1984, 1998). When the desktop revolution forced them to embrace digital systems, they were already vulnerable to data breaches although this was not widely acknowledged (Brancheau & Brown, 1993). The problems were further exacerbated with the coming of the World Wide Web and e-commerce (Henson & Kuzma, 2010).

The first widely acknowledged standard in this area (BSI, 1998), evolved from a quiet acknowledgement at government level that 100% security based merely on encryption (e.g. the US 56-bit DES standard) was not possible. Such an acknowledgement would not have been popular, and was of course not officially stated until much later (George, 2012). A systematic, workable information assurance scheme was a natural next step beyond a product-based solution. By the late 1990s, large organisational digital systems were already complex and multinational. A new UK standard, BS7799, (BSI, 1998) was initially developed with large organisations in mind, using the concept of the Information Security Management System (ISMS). As it became more widely accepted that management of information risk and having an effective ISMS were critical factors on information security, BS7799 was badged as an Information Assurance Standard. It was widely adopted outside the UK and was further developed by a committee of ISO (International Standards Organisation) to become an International Standard, ISO27001 (ISO, 2005).

Nothing anything like equivalent had been developed for SMEs, who were historically not online anyway. It rapidly became apparent, however, that, with the further development of the Internet, SMEs were being encouraged to become part of a networked digital supply chain, and therefore could not be ignored on the basis of smallness. Some SMEs would have tried to engage with information security "as a product" but would have been frustrated by the impossibility of achieving their goal. Yet there was no realistic information assurance for them because ISO27001 and other long-standing IA standards such as COBIT (Control Objectives for Information and Related Technologies) (ISACA, 1996) were written for a "large organisation" mindset.

By 2007, the principles of information assurance were well understood by large organisations and government although most sought the less robust "compliance" solution rather than audited certification against benchmarks. In Europe, ENISA was aware that small businesses would not find the ISO27001 information risk management process helpful and developed something more workable (ENISA, 2009), but ISO27001 is large and much of the required documentation was still way beyond the resources available to an SME. Therefore, except in rare circumstances, SMEs and Information Assurance just didn't seem to mix.

The problem has been addressed in a number of ways in recent years. The first UK-based development was the pilot IASME scheme (Henson & Booth, 2010), which used the principles enshrined in ISO27001 in a more SME-friendly way. IASME still needed time and resources to implement, however, and SMEs would not necessarily see this as critical to the survival/growth of their business. It is also possible that the earlier view of information assurance associated with ISO27001 and COBIT has persisted with SMEs and advisory organisations like FSB and Chambers of Commerce.

In previous papers, one of the authors has argued for broader policy changes at government level (e.g. stricter laws) to help impress upon SMEs the need to raise their game regarding information security, or even more subtle methods such as the introduction of cyber liability insurance with premium levels tied to

demonstration of at least base level security (Henson & Sutcliffe, 2013), but at that time there was still disagreement about such matters as what constituted "base level" security. Happily, this was resolved, in the UK at least, with the introduction of Cyber Essentials by CESG, the information assurance wing of GCHQ the following year, in 2014 (CESG, 2014).

Our aforementioned 2015 paper identified that many UK SMEs did understand legal implications of neglecting security and were prepared to spend more, but did not have sufficiently clear guidance on the best way to go because they were suspicious of even the term Information Assurance, which was a concern in itself.

Information Assurance in the SME Space in 2016

The evolution of IASME, PCI-DSS and other schemes into Cyber Essentials, launched in 2014, was a big step forward welcomed by many in the industry, and the low cost of a self-assessed scheme was thought to also address the concerns of financially pressed small businesses. This, as well as the increased reporting of cyber security breaches in the media, was discussed in the earlier paper, and it was therefore hoped, even anticipated, that SMEs would be interested in getting a badge to show they had at least "base level" security as defined by government experts. The 2015 data showed a slightly disappointing take up of Cyber Essentials but it was accepted as being early days for the scheme.

In Europe, new legislation relating to personal data had been debated since 2012, and came to fruition with the Digital Single Market (EU, 2015) and the GDPR (General Data Protection Regulation) (EU, 2016). All this was well known to UK business organisations, and developments were regularly reported in business and computing media. Moreover, in the UK Cyber Essentials became mandatory in the Ministry of Defence supply chain from January 2016 (HMG, 2016). It might therefore have been expected that in the UK Cyber Essentials would become very successful.

However, according to secondary data from the four awarding bodies (IASME, 2016; CREST, 2016; QGMS, 2016; APMG, 2016), the SME demand for Cyber Essentials, a base-level, minimum cost, and mostly technical information assurance scheme, so far is still disappointing. The exact figures are extracted from the certification bodies own websites and are included in Fig. 1 below. As can be readily seen, the exact total on 16th June 2016 from all four certification bodies was 1688.

Figure 1. *Number of Cyber Essentials certificates awarded by 16/6/16*

Certification Body	Total Cyber Essentials & CE-plus certificates awarded
CREST	540
IASME	777
QMGS	352
APMG	19
TOTAL	1688

However, the raw figures don't tell the whole story. Looking at individual figures for certification bodies, some of those certificated are larger, public sector organisations, others are charities, and some organisations are included twice (a second time for Cyber Essentials Plus, which is a more robust next step for information assurance). The actual figure for SMEs is therefore far lower. There are currently 5.382 million SMEs in the UK (UK Parliament, 2015), and the number is still growing. The implications of the Cyber Essentials figures in this context are discussed in the final section of this paper, along with results of the attitudinal studies.

Research Hypotheses

According to our 2015 survey the term "Information Assurance" seemed to be putting SMEs off and perhaps that was an important contributor to the continuing enigma of lack of SME investment in cyber security in spite of the very well documented evidence that they were vulnerable and under threat. The purpose of this study is to examine this effect in more detail and suggest possible ways forward for SMEs, and to protect the rest of UK information infrastructure.

The hypothesis strongly supported in last year's study was:

"SMEs have a negative attitude towards Information Assurance"

If they already have a negative attitude to Information Assurance, they will probably avoid it, and that does seem to be borne out in Cyber Essentials statistics. The purpose of this study is to prove/disprove whether it is true that SMEs do still have a negative attitude to different aspects of information assurance. The intention of this study is to look deeper into what is discouraging businesses from getting Information Assurance certification, even if self-certified.

As with last year's study, the research questions to establish attitudes have been divided into a number of categories:

"H1: Are Information Assurance standards needed for the small business?"
It may be that the whole concept of standards is not considered to be relevant to improving security, as far as many SMEs are concerned.
"H2: Are Quality Assurance standards an important factor in choosing an Internet Service Provider (ISP)?"
There is evidence that small businesses have not been encouraged to use "due diligence" in choosing a business partner for their Internet access and/or to provide them with a web site, and are therefore very vulnerable to attack through this route. To what extent is this really true?
"H3: Is Information assurance not regarded seriously as a way of improving security, but more cynically as a way for information security consultants to get at their money?"

Many services are on offer to small businesses. Small businesses can perhaps be forgiven for thinking that those offering to provide a security service, rather than a product, are not offering good value for their often limited and tightly controlled finances.

> "H4: Have they previously heard of "Cyber Essentials", and now they have, do they see this as a useful solution to basic cyber security problems with SMEs"

Cyber Essentials was introduced with plenty of enthusiasm, but the lack of SMEs that have even heard of this benchmark shows the continuing lack of SME interest in this space.

> "H5: Have they previously heard of "IASME", and now they have, do they see this as a useful solution to basic cyber security problems with SMEs"

If many SMEs haven't heard of Cyber Essentials, probably even more are not aware of IASME, as a next step beyond acquiring basic security controls. The fact that IASME also includes an option for third-party auditing and scrutiny of people controls at much lower cost than ISO27001 may therefore not have registered with SMEs.

Through the data supplied by SMEs in response to these questions, the researchers will seek to improve current understanding of how an apparently information assurance-adverse SME mindset persists, and postulate possible strategies for changing it.

Methodology

Either face-to-face structured interviews or on-line questionnaires were the possibilities considered. Given the geographical distribution of respondents and online was considered to be the best approach.

Research data was gathered online, and it was agreed that a SurveyMonkey questionnaire allowing selection of 1-5 for each question would be used.

The hypotheses would be tested through a set of 26 online questions divided into five categories corresponding to the five hypotheses. These would be put to SME senior managers via the online questionnaire. Using accepted guideless for writing attitudinal surveys (Lewis & Seymour 2004), the questions were designed to be carefully worded to address one or other of the hypotheses and divided appropriately into the five above categories. Each question related directly to the specialised theme of "Why are SMEs suspicious about using Information Assurance to help improve their cyber security?" and was also designed to contribute to a broader picture about SMEs and systematic use of security controls and ISMSs.

A similar technique would be used for circulation to that employed last year, but using a client-base that was specific to two regions supported by the

same chamber of commerce (Herefordshire and Worcestershire). Lessons learned from that survey were applied 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), and the local Chamber of Commerce were also helpful in this respect. The reason for excluding IT managers is that, as middle management, they rarely have much influence on the culture of the organisation.

The questionnaire was designed online with mostly closed questions for ease of analysis. Different pages were included for different lines of questioning. The content was revised until both researchers were happy that all ambiguities had been removed, and can be viewed directly at URL: https://www.survey monkey.co.uk/r/LQPSVCV

Questions were constructed so that some had a response of "5" as most negative, whilst others were "1" for most negative. This would ensure that a respondent with a motive to be deliberately "positive" or "negative" couldn't just go down the list ticking first or last boxes. This extra feature meant that analysis was slightly more difficult, but the researchers considered it to be important if the data obtained was to be reliable.

Implementation of Methodology

The URL was distributed to senior management of a random selection of SMEs via email. The SME respondent had to provide a response between 1 and 5 according to a Likert scale for each of the 26 questions. Some general questions such as business size and sector were also included. The incentive for completing the questionnaire was entry in a prize draw for two half-days free consultancy towards the Government-recommended Cyber Essentials (CE) or CE-plus.

The email lists used were from the SME contacts of a regional UK Chamber of Commerce. The appropriate person in each SME was contacted, and a random subset of responses was obtained.

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

- How many employees?
- What sector?
- How do you manage your data?

The 26 questions focusing on attitudes to information assurance are included as appendix 1.

Treatment of Spreadsheet Results

Survey Monkey captures the raw data, and then provides statistical data for each individual response, on an Excel spreadsheet. The spreadsheet data was

kept confidential, although no SME names were required to complete the questionnaire.

Overall data covering all of the individual 26 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 to score "5" as showing the most negative attitude:

- An ISP just provides a connection to the Internet. Standards are only about cabling, etc. and shouldn't be a factor in choosing.
- There are too many standards and this is stopping businesses from growing
- Standards have no place in the modern digital economy
- Standards should not be applied to management practices
- I've heard it can cost £10K or more for a business to get ISO27001 certified, and any other standard is likely to be quite expensive for my business
- The requirements for getting a Cyber Essentials badge make it too expensive for most small businesses
- Other businesses don't really care whether we've got evidence that we take cyber security seriously
- If we get a breach our reputation will be tarnished whether or not we have Cyber Essentials, so why bother?
- I don't think Cyber Essentials is relevant to businesses like mine
- I don't think IASME is relevant to businesses like mine
- A standard mostly about technical controls protecting data is all I'm likely to need (x2)

Actual scores had 3 subtracted and sign reversed to get the Standardised scores. The following questions had "1" as showing a negative attitude:

- Standards are important for the small business
- Standards are vital to engineering, and therefore for technological development
- Standards are there for a purpose, and they make business work more efficiently
- An ISP is essential for any modern business and all factors should be considered
- An ISP that doesn't have evidence of quality assurance is more likely to be unreliable
- Information assurance certification shows that the ISP takes security seriously, and this matters greatly to me
- I would pay more for an ISP that can show audited evidence that they are keeping my data secure

- Cyber security professionals are only trying to help SMEs get to an appropriate standard to protect their data, and get a bad press
- Cyber Essentials may help the business identify insider cyber security problems
- Cyber Essentials may help the business resolve insider human threat problems

This time, actual Scores had 3 subtracted from them to get the standardised scores.

Collective Results

Averaged positives and negatives for each of the 26 questions were collectively included in categories as appendix 2.

The raw results would have to be "standardised", using the method described in paragraph 8.1. In order for any of the five hypotheses to be supported, the normalised scores for that category would probably need to have an averaged value somewhere between 0 and +2. Averaged scores of between 0 and -2 would suggest that the hypothesis is not supported. Whether or not this was the case is shown in the next section.

Analysed Raw Data

Results per question: (see appendix 1)

Results by category, including number of 5=negative and 1=negative questions (actual results presented in appendix 2)

Table 1. *Grid for analysing Questions by Category*

Category (based on hypotheses)	Breakdown of 1=negative to 5=negative questions	Overall rating (>0 for each pos attitude <0 for each negative attitude)
"H1: Are Information Assurance standards needed for the small business?"	3 questions 5 for neg attitude	
	3 questions 1 for neg attitude	
"H2: Are Quality Assurance standards an important factor in choosing an Internet Service Provider (ISP)?"	1 questions 5 for neg attitude	
	4 questions 1 for neg attitude	
"H3: Is Information assurance not regarded seriously as a way of improving security, but more cynically as a way for information security consultants to get at their money?"	4 questions 5 for neg attitude	
	1 questions 1 for neg attitude	

"H4: Have they previously heard of "Cyber Essentials", and now they have, do they see this as a useful solution to basic cyber security problems with SMEs"	3 questions 5 for neg attitude	
	2 questions 1 for neg attitude	
"H5: Have they previously heard of "IASME", and now they have, do they see this as a useful solution to basic cyber security problems with SMEs"	3 questions 5 for neg attitude	
	2 questions 1 for neg attitude	

Summary

- Hypotheses well supported for four of the five categories. These SME responses show that they do understand the problems facing them regarding information security, and understand that information assurance solutions appropriate to their needs are available.… they just have problems going that next step and taking the action that experts consider necessary
- A fifth category i.e. "Information assurance is just another way for those ruthless security people to get money out of the small business" also got a positive response.

This was perhaps too small a positive score to be statistically significant, but suggests that many SMEs are not happy with solutions typically offered by security professionals via information assurance. They seem to perceive such solutions as excessive, time-consuming, and an unwelcome ongoing expense.

Discussion of "Normalised" Results

The data obtained for four of the categories, averaged out, shows an overall response to the questions that is very positive. This confirms an overall highly positive response to the system that has evolved to assist the small business with information security.

However, the considerably negative response to the questions in the third category relating to information assurance standards (pitched to support a "negative attitude" hypothesis) is certainly worthy of further investigation. The process of obtaining a standard, badge, or Kite mark happens without fuss in many industries. The previously expressed observation (Henson & Garfield, 2015) that SMEs do not give due recognition in terms of securing their own and customers' data should now be seen in the context of the accepted process for getting such benchmarks, etc. and how it impinges on the important matter of running the business. There is much more work that needs to be done to explain why such thinking should be widespread amongst SMEs.

Evaluation

The hypothesis identified in our 2015 paper that SMEs have a negative attitude towards information assurance is not reinforced by our findings in 2016, but the process required to get information assurance certification does evoke a negative response. The further investigations have also demonstrated that activities related to information assurance, and therefore part of the process, are not regarded as of importance by SMEs. There is a bit of a contradiction here because there is plenty of evidence to suggest that SMEs are regularly getting caught out in this area (Henson & Moore, 2015) but businesses do not take notice until they have personal experience of this.

The other aspect of the current research – the secondary data taken from Cyber Essentials certifications to date – shows a very low take up of information assurance certifications devised particularly to meet the needs of SMEs. Relating this to outcomes of our own primary research, the negative attitude to accepted information assurance practices and those who advise on them, the nature of the problem becomes apparent. SMEs are unlikely to be seeking to manage their information security and get certified against industry agreed standards - because they, remarkably, still view information assurance processes and those who put them into practice - with suspicion. They seem not to see cyber attacks as a real and present danger to their business, and disregard statistics that consistently confirm this danger, probably because they also view the sources of this data with suspicion. It seems that a campaign is needed to improve the standing of cyber security professionals with SME owners. How this is can be achieved can only be speculated about but some possible solutions have been tried to a limited extent and are presented below:

1. Cyber Insurance
   This was discussed in a previous paper (Henson & Sutcliffe, 2013). As with information assurance, the take up by SMEs in the UK has been consistently low
2. Offering better safeguards through Regulation
   In the absence of compulsory GDPR it is doubtful whether what will be perceived as other countries laws will have limited positive effect on UK SMEs
3. The fall-out from an increased number of high profile information breaches from 2015, and a change of reporting of crime statistics to include cyber crime may in time raise the issue of keeping data safe and secure with SMEs to "critical mass"

These factors are all potentially positive, and, several weeks ago, this paper might have been more optimistic regarding the effect of GDPR on UK SME cyber security. However, the remarkable decision of the British people on June 23rd 2016 to, by a narrow majority, for Brexit (Dorling, 2016) means that GDPR will not become law in the UK. Whilst the UK government does have its own Cyber Security strategy (HMG, 2011) its implementation is considerably

dependent on collaboration between EU partners, and here will probably be an increasing dependence on organisations like FSB and Chambers of Commerce to keep SMEs appropriately informed at a local level. This would assume that these local organisations are themselves well-informed about the benefits of information assurance as an accepted best strategy for improving information security, and there is evidence that work needs to be done in this area.

It would be interesting to compare SMEs in the UK with those of the other 27 EU states in the coming years to see whether the "Brexit" decision, if it is carried forward, will have a negative effect on UK SME progress towards adopting information assurance practices, and the best measurement at the moment is uptake of Cyber Essentials certificates. Any slowing down would clearly not be a desirable effect for UK business.

Conclusion

Attitude changes require a change in perception. What is happening in business is merely a subset of what is happening in wider society. The digital revolution has already happened and seems to have brought about a cultural divide between those willing to embrace it and those who hark back to a bygone age when business activities happened face-face. The message behind GDPR was quite clear, and explicitly put… the roll out of the Digital Single Market in Europe by 2018 is an essential part of the marketplace which will be more and more digital as commerce and other aspects of our culture embrace the information society. The obvious way to secure data as that new infrastructure unfolds is to employ proven best practice in cyber security, and whether SMEs like the term or not, that means information assurance.

Like any new practice as a result of social change, information security can only progress if the public are prepared to buy in to best practices that provide an effective solution. One year on from our last research, desired public perceptions that (a) cyber crime is increasingly hitting small businesses and (b) this really matters because businesses with data breaches are more likely to fail still do not mesh with reality and therefore do not mesh with small business. Last year, based on our findings, we suggested a potential (but unlikely) consequence of overseas trading that we

> "… 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."
> (Henson & Garfield, 2015, p.13)

As already stated, the potential "game changer" of EU regulation, seems more distant in terms of transforming UK SME practice than one year ago. The reality of Brexit may indeed encourage UK PLC to join up its own thinking more urgently regarding an effective implementation of its Cyber Security Strategy.

The EU model for a Digital Single Market seems likely to be a template of good practice for many areas of the world, and for the UK to be successful in trading practice UK businesses will need to be seen to be embracing GDPR. Whatever has happened before, the wise EU states will be in competition with each other to have the best record on SME cyber security and tackling cybercrime, and a wise UK would need to embrace this new reality. An enhancement of the 2011 UK Cyber Security Strategy to align with the EU Strategy and embrace the DSM seems the best way forward and Cyber Essentials provides a workable vehicle to drive this forward but evidence on the ground and from perceptions show continued SME reticence about using information assurance. According to the data this is at least partly because they are suspicious of costs, including fees of the security professionals who are purporting to support them. EU policy will drive the digital single market across EU states, and UK SMEs need evidence of good information assurance to compete in this market, so a solution to this problem needs to be found. If SMEs refuse to pay, the price should be lowered… either through subsidy or through add-ons such as cyber security.

Glossary

BIS	UK Government: Department of Business Innovation & Skills
BSI	British Standards Institute
COBIT	Control Objectives for Information and Related Technologies
DSM	Digital Single Market
EU	European Union
FSB	Federation of Small Businesses (UK)
GDPR	General Data Protection Regulation
IA	Information Assurance
IASME	Information Assurance for SMEs
ISMS	Information Security Management System
ISO	International Standards Organisation
PCI-DSS	Payment Cards Industry Data Security Standard
SME	Small and Medium-sized Enterprise

References

Arthur J, 2009, “Information Security survey of SMEs for Worcester Business School” [online at http://staffweb.worc.ac.uk/hensonr/Information% 20Assurance %20Market%20Research%20v3JAAB.ppt]

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]

BSI, 1998, “BS 7799-2:1998 Information security management. Specification for information security management systems”

CREST, 2016, “Cyber Essentials Certified Companies”, [online at http://www.cyberessentials.org/list/]

Dordick, HS, Bradley HG, Nanus B, Martin TH, 1979 “Network information services” *Telecommunications Policy*, Volume 3, Issue 3, Pages 217-234.

Dorling, 2016, “Brexit: the decision of a divided country”, BMJ 2016; 354:i3697 [online at http://www.bmj.com/content/354/bmj.i3697.full] 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, 2005, “SME definition: User guide and model declaration” [online at http://ec.europa.eu/enterprise/enterprise_policy/sme_definition/sme_user_guide.pdf]

EU, 2013, “Cyber Security Strategy: An Open, Safe and Secure Cyberspace”, https://ec.europa.eu/digital-single-market/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace”

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

EU, 2015, “A Digital Single Market”

EU, 2016, “General Data Protection Regulation” [online at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN]

EU, 2016, “Digital Single Market: Cybersecurity” [online at https://ec.europa.eu/digital-single-market/en/cybersecurity]

Fomin VV, 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]

George, R., (2012), “The Evolution of Information Assurance”, 21st Usenix Security Symposium, Bellevue, Washington State, USA, August 8-10th 2012, [online at https://www.usenix.org/conference/usenixsecurity12/evolution-information-assurance-0]

Goucher W, (2011), “Do SMEs have the right attitude to security?” Computer Fraud & Security Volume 2011, Issue 7, July 2011, Pages 18–20.

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

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 & Moore L. (2015), "Anatomy of a Cyber Attack", Computer Weekly, June 2015, [online at: http://www.computerweekly.com/feature/Anatomy-of-a-cyber-attack-the-risks-facing-small-businesses]

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

HMG, 1984, "Data Protection Act (1984)", Her Majesty's Stationary Office.

HMG, 1998, "Data Protection Act (1998)", Her Majesty's Stationary Office.

HMG, 2011, "UK Cyber Security Strategy", Her Majesty's Stationary Office.

UK Parliament, 2015, "Business Statistics", p5. [online at http://researchbriefings.files.parliament.uk/documents/SN06152/SN06152.pdf]

HMG, 2016, "MOD Implementation of Cyber Essentials Scheme" [online at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/494608/ISN_2016-01_Implementation_of_Cyber_Essentials_Scheme-O.pdf]

IASME, 2016, "Certified Organisations", [online at https://www.iasme.co.uk/index.php/companies-certified]

ISO, (2005), ISO/IEC 27001:2005, International Standards Organisation.

Lewis E, & Seymour E, 2004, "Fieldtested Learning Assessment Guide", 2004 [online at http://www.flaguide.org/extra/download/cat/attitude/attitude.pdf]

Ponemon Institute, 2016, "2015 Annual Study: UK Cost of a Data Breach", PGP Corporation.

QGMS, 2016, "Cyber Essentials Certified Companies", [online at http://www.qgstandards.co.uk/cyber-essentials-accredited-companies/]

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. *Individual Results*

"1" as negative attitude

Standards are important for the small business	+1.4
Standards are vital to engineering, and therefore for technological development	+1.1
Standards are there for a purpose, and they make business work more efficiently	+1.2
An ISP is essential for any modern business and all factors should be considered	+1.2
An ISP that doesn't have evidence of quality assurance is more likely to be unreliable	+0.55
Information assurance certification shows that the ISP takes security seriously, and this matters greatly to me	+1.3
I would pay more for an ISP that can show audited evidence that they are keeping my data secure	+0.45
Cyber security professionals are only trying to help SMEs get to an appropriate standard to protect their data, and get a bad press	+0.45
I'd not previously heard of Cyber Essentials, the government's new Information Assurance scheme targeted at SMEs, before starting this questionnaire	+1.3
Cyber Essentials may help the business identify insider cyber security problems	+0.45
Cyber Essentials may help the business resolve insider threat problems	+0.5
I'd not previously heard of IASME, the government's new Information Assurance scheme targeted at SMEs, before starting this questionnaire	+0.15
IASME may help the business identify insider cyber security problems	+0.85
IASME may help the business resolve insider threat problems	+0.8

"5" as showing a negative attitude

There are too many standards and this is stopping businesses from growing	+0.1
Standards have no place in the modern digital economy	+1.7
Standards should not be applied to management practices	+1.1
An ISP just provides a connection to the Internet. Standards are only about cabling, etc. and shouldn't be a factor in choosing	+0.9
I've heard it can cost £10K or more for a business to get ISO27001 certified, and any other standard is likely to be quite expensive for my business	+0.25
The requirements for getting a Cyber Essentials badge make it too expensive for most small businesses	+0.55
Other businesses don't really care whether we've got evidence that we take cyber security seriously	+0.6

If we get a breach our reputation will be tarnished whether or not we have Cyber Essentials, so why bother?	+0.5
A standard mostly about technical controls protecting data is all I'm likely to need (Cyber Essentials)	+1.0
A standard mostly about technical controls protecting data is all I'm likely to need (IASME)	+0.75
I don't think Cyber Essentials is relevant to businesses like mine	+0.75
I don't think IASME is relevant to businesses like mine	+1.0

Appendix 2. *Category Results*

Hypothesis	Calculation from questions	Category Score
"H1: Are Information Assurance standards needed for the small business?"	Sum of 5 neg… +3.2 Sum of 1 neg… +3.7	+6.9
"H2: Are Quality Assurance standards an important factor in choosing an Internet Service Provider (ISP)?"	Sum of 5 neg… +0.9 Sum of 1 neg… +3.5	+4.4
"H3: Is Information assurance not regarded seriously as a way of improving security, but more cynically as a way for information security consultants to get at their money?"	Sum of 5 neg… +1.75 Sum of 1 neg… +0.45	+2.2
"H4: Have they previously heard of "Cyber Essentials", and now they have, do they see this as a useful solution to basic cyber security problems with SMEs"	Sum of 5 neg… +2.7 Sum of 1 neg… +0.95	+3.65
"H5: Have they previously heard of "IASME", and now they have, do they see this as a useful solution to basic cyber security problems with SMEs"	Sum of 5 neg… +1.3 Sum of 1 neg… +1.65	+2.95