Information Assurance and SMEs: Research Findings to inform the development of the IASME model

Richard Henson, Senior Lecturer in Computing and Knowledge Transfer Fellow in Information Security, University of Worcester
David Booth, CESG Senior Consultant (retired).

1. Abstract

This paper reviews the research findings of the University of Worcester on SMEs in 2009 and looks at other recent academic and corporate research on SME data security in the EU and the rest of the world exploring the unique problems faced by SMEs in securing information. It illustrates the importance of SMEs in the national business infrastructure, and shows that there are significant shortfalls in the protection of SMEs from cyber attack, affecting both their viability and the security of the data which they hold in relation to the larger businesses and government organisations who are often their main customers.

After providing considerable evidence to demonstrate the current size of the problem, and the difficulties involved for SMEs to implement certification to the International information security management standard ISO/IEC 27001, this paper goes on to introduce the Information Assurance for SMEs (IASME) process as a possible solution for SMEs in terms of a customised implementation of ISO/ IEC 27001 that is more achievable and more appropriate to the business needs of the SME. This process has been developed over the last 12 months with the cooperation of a number of SMEs providing input on relevance and implementation and is contained in the IASME Standard document.

2. Introduction

Nowadays, whether large or small, publicly floated or privately owned, a business **is** its information. All businesses therefore need to make it a priority to take appropriate safeguards to protect their information. This has been recently emphasised by the UK National Security Strategy published October 2010 which places information security in Tier One, or most important risks to the UK. It says in part that “In particular, protecting virtual assets and networks, on which our economy and way of life now depend, becomes as important as directly protecting physical assets and lives”.

Extract: Like terrorism, this is not simply a risk for the future. Government, the private sector and citizens are under sustained cyber attack today, from both hostile states and criminals. They are stealing our intellectual property, sensitive commercial and government information, and even our identities in order to defraud individuals, organisations and the Government.

As electronic information systems have developed, efforts to provide support for information security have mainly followed a "big business" model. Also, most of the academic and private sector research on information security in organisations has focused on the public sector or larger private enterprises. Yet it has been long acknowledged, most recently by Backhouse et al. (2006), that smaller businesses, or SMEs (small and medium-sized enterprises), do not behave in the same way as larger organisations regarding information systems and their management. They should therefore not be treated in the same way as regards advice on their protection of information assets

3. The Information Security Problem with SMEs

3.1 What is an SME and why do SMEs matter?

There are at least three different definitions of SME in different parts of the world, which does cause confusion. Also, in the US there is a similar term SMBs (small and medium sized businesses) with small as 1-100, and medium as 101-1000. However, this study will focus on the long-established and recently revised EU definition (EU, 2005), which refers to an SME as a company that employs up to 250 employees. Micro businesses have 1-10 employees, small businesses are defined as 0-49 employees, and medium sized enterprises comprise 50-249.

According to recent government figures (BERR, 2009), numbers of SMEs in the UK continue to grow, to the remarkable figure of 99.9% of all British companies! The same figures show that SMEs make up 59.4% of UK private sector employment, more than 50% of the UK GDP (Gross Domestic Product) and that they are responsible for approximately half of UK turnover. Perhaps to clarify any possible confusion, the SME figures also break down further to show figures separately. For example, the numbers of small and medium sized enterprises compared to all private enterprise are 99.3% and 0.6% respectively.

3.2 Why are SMEs so important to National Information Infrastructure?

National Information Infrastructure could be regarded as the many ways that digital information gets transported electronically between organisations, including SMEs, large private sector, and public sector organisations. Transport media are usually through either copper-based or optical fibre-based cable systems, but wireless systems are also used. Quite a lot of this information is subject to legal protection, and it is important that such information is appropriately labelled and given due protection using one of more of the methods available. The methods available are explained later in this report.

Not only do SMEs make up a substantial amount of UK trade, but they also link in directly to larger companies and public sector organisations. Figures obtained in the West Midlands (Adroit Economics, 2007) show that only about two-thirds of SMEs are connected to the Internet. Even so, that means about

66% of the nodes that make up the national information network for doing business is likely to be SMEs! The authors suspect that in 2010 this proportion is considerably higher.

Many businesses provide products and services to other businesses, and in this modern, connected world, that means that enormous amounts of information will be shared via the internet and stored on SME IT systems. The information security needs of SMEs are therefore just as important to the nation as those of larger organisations. It is quite remarkable that, to date at least, there seems to have been little effort to assist this massive slice of British business to protect their information assets beyond providing useful, but relatively introductory advice on government-funded websites. There is little, for example, about how to manage information security using an information security management system (ISMS). A major aim of the IASME project seeks to combine the principles of the International Standard and research into the actual workings of information systems of small businesses to develop and implement a model for serving those needs.

3.3 What is happening to support The National Information Infrastructure?

As explained later in this report, much of the national infrastructure for conveying digital information is provided by the Internet. Advice provided on doing business online therefore tends to focus on aspects of using the Internet. However, it is one thing to provide information on a topic, and quite another to put it in context. Businesses reading general advice on online trading provided by reputable national bodies could be forgiven for thinking that information security was an optional add-on, and nothing to lose any sleep over. In fact, the threat to their data, and therefore their business, is very real. Recent world-wide research (e.g. Verizon, 2008, 2009a), shows that about one third of data breaches covering millions of records occurred through vulnerabilities in partners systems! Research is available from many other sources besides Verizon, and they show similar patterns. It seems implausible that British businesses would be significantly different from other developed countries.

The only British website of prominence that gives a clear impression of a threat environment is that of the Information Commissioner's office (ICO, 2010a). In recent years, the ICO has been seen by some as "piggy in the middle" between a UK government reluctant to bring in new legislation and a EU keen to encourage the UK government to toughen its data protection laws. At least one prominent UK privacy lawyer has publicly shown sympathy with the EU position (Computer Weekly, 2010), and the ICO has very recently released a statement encouraging debate and suggesting possible sympathy with the EU on this matter (ICO, 2010b). It therefore appears that a further tightening of the law is at least possible, and this can only happen satisfactorily if SMEs have a range of advice and information open to them. As David Lacey has rightly pointed out in his recent review for the ICO of currently available SME advice on information security (ICO, 2010), many publicly-funded websites are either introductory, out of date, or both.

If statistics such as those provided by Verizon could receive sufficient publicity in the SME space, they may well help businesses to accept their responsibility and take information assurance more seriously, and this may have a knock on effect across the supply chain. One aim of the IASME project is to keep businesses well informed through its website (IASME, 2010) and it also aims to provide links to up-to-date and reliable statistics that will give SMEs a realistic impression of the potential threats to their and business partners data, and allow them to make up their own minds what they should do about it.

Another driver for SMEs has been observed during the IASME pilot. Even though many larger organisations remain naïve about their own security, there is an increasing trend for larger clients to demand that SMEs look after their information in a secure fashion where this is part of the business relationship.

3.4 Why is it that even large companies experience problems with Information Security?

The matter of adequately securing electronic information assets goes back to the time that digital information came out of the mainframe and started appearing on the desktop. A recent historical study (Henson & Kuzma, 2010) documents how academic researchers highlighted potential problems with security as the processing of digital information came away from the mainframe and onto the desktop. However, academics do not control the purse strings of organisations, and they did not really get to grips with the problem in a structured and influential way until 2001 when Ross Anderson of Cambridge University wrote a seminal paper with far-reaching consequences (Anderson, 2001). The following year, Ross and another influential writer and researcher, Bruce Schneier, debated head-to-head the matter of organizational spending on safeguarding information assets (Anderson 2002; Schneier, 2002), and founded the discipline of “Economics of Information Security”.

WEIS (Workshop on Information Security) rapidly became influential with decision-makers in large organisations. A number of issues have been identified in recent years which could act as a possible driver/barrier for the ISMS development process, and to motivate businesses to spend on information security related matters. They are listed below:

I. Legal and Regulatory (avoiding fines)
II. Protection of Reputation and Brand (loss of market share)
III. Physical Cost of a Data Breach
IV. Loss in stock market value if a breach is publicized (not SMEs)
V. Insurance premiums (higher as a result of data breach)

Factors tending to make investment in information security apparently less important have been:

VI. Outsourcing IT and information storage to third parties
VII. Outsourcing IT and information storage to the 'cloud'

Although there is a debate raging on the efficacy of this kind of outsourcing, it cannot reduce the effect on the business of losing confidentiality, integrity or availability of their data, as the outsourcing facility is unlikely to recompense the business in the event of failure. What they can do is move the cost centre and risk focus but this is often poorly understood by the business. Furthermore, and unfortunately for SMEs, most researchers in this new discipline have focused their efforts on the information assets of larger organizations. In the final session of WEIS 2009, minuted in the workshop blog (Anderson, 2009), Henson made a plea to the research community to focus more on the gathering of financial data that could encourage small businesses to improve their information security.

4. A Review of Available Research since the introduction of an International Standard on information security

4.1 A review of Academic Studies

The ICO commissioned a study on SMEs in 2003 (ICO, 2004). It was conducted by an academic research group (ERDU) based at the University of Lincoln, and focused on attitudes to security. The conclusions of this study seem somewhat optimistic in the light of later work, as a survey commissioned by the ICO three years later showed that, in a sample of 813, "only 22 per cent of SMEs surveyed were aware the Act requires them to keep customer information accurate and up to date." (ICO, 2007). The results of this survey were released shortly before the HMRC disaster where 26 million records went missing.

ISO27001 (initially BS7799) was launched as a standard for information security management as a means of (amongst other things) putting plans into action, which would help to ensure that high management ideals on data protection were put into place with real digital information. It was generally welcomed, but a note of caution was sounded through some significant SME research that was being undertaken at the time (Coles-Kemp & Overill, 2007). Whilst acclaiming the introduction of a standard, the authors suggested that the ISMS model presented in ISO27001 was perceived as too complex by typical SMEs, and that a simpler model was needed, which would more easily embed the ISMS within existing business processes.

A small number of private sector and academic studies conducted since the introduction of the International Standard have more directly asked SMEs questions relating to their Information Security. Most of the academic studies have been conducted outside the UK but the private sector studies all have at least some British data. In any case, the matters raised, discussed, and examined would seem to echo the concerns expressed by, and about, SMEs within the UK. The most pertinent of these studies are discussed in this paper, and all those scrutinized and are considered relevant to the purposes of IASME are listed in Appendix 1 at the end of this document.

An Australian study (Dojkovski, S, et al, 2007) looked at information security in the context business culture, and researched management challenges in nurturing greater information security awareness among employees. It is interesting to note here that there was not mention of standards, or encouragement of Australian SMEs to aspire towards ISO27001. However, it is also interesting to that the Australian and New Zealand governments had by then already developed their own joint standard, AS/NZS4444 based on BS7799, which was subsequently superceded by the ISO standard. Yet 29 ISO27001 certificates have been awarded to date in Australia, compared to 444 in the UK. It seems difficult not to conclude that Australian SMEs are showing little interest in developing information systems management systems.

One detailed academic study on SMEs of that same year was conducted in Germany (Kluge et al, 2008). A large number of organizations were contacted, and the response rate was 5%. The responses revealed the dilemma of SME's in today's business environment with the expectation that information is managed electronically. Here is one example:

"Practically all responding companies stated that their company IT was business critical to them (96%) but only a small part of them (17%) had a written IT security policy in place."

(Kluge et al, 2008, p.7)

The number of ISO27001 certificates awarded in Germany is currently showing signs of growth, to 137. This is still much lower than the UK, however, which has a lower overall business population.

Another study of European businesses was conducted the following year (Barlette & Fomin, 2008). It focused not just on SMEs but on all businesses, working on the pretext that there might be a similar pattern of growth to that shown for ISO9001 several years earlier. Their findings were summed up effectively in the abstract:

"In this paper we examine the adequacy of IS security standards to the needs of SMEs. Using the findings of literature review, we identify general criticism for the security standards. Further, we benchmark the recently published ISO 27001 IS security standard to ISO 9000 standard - a similar standard with a 20 years history - to develop expectations of how the future adoption of the recently introduced ISO 27001 standard can be fostered. We suggest, among other, that the legislative environment can play a crucial role for further growth of security standards adoption."

(Bartlette & Fomin, 2008, abstract)

This study confirmed Coles-Kemp & Overill's fears about ISO27001, but clearly identifies legislation as having a crucial role in future encouragement of SMEs to work towards the standard. The follow-up study published later the same year (Fomin et al, 2008) look at possible reasons for the disappointing uptake of the ISO27001 in the Netherlands, but a deeper analysis shows that a lot of companies purchased the Dutch version of the standard; in fact, ISO2700l has been translated into many tongues and it seems unlikely that language should be a barrier if management provides direction and backing. One interesting recent study from Korea (Lee and Yang, 2009) provides a much more thorough analysis of human, technical and human aspects of embedding information security, and provides management guidelines for successful protection of information assets.

Perhaps the detailed and logical Korean guidelines are better suited to an Asian business culture where PDCA (Plan-Do-Check-Act) principles are more readily understood. Henson & Hallas (2009) took the ISO27001 comparison across nations further and used the centrally available statistics available from the ISO 27001 body to contrast Western European usage of ISO27001 with Pacific Rim countries. Their findings showed that not only were the Asian businesses powering ahead with developing information systems to the International standard, but also the gap with European countries was widening as European GDP fell into recession. The paper identified cultural reasons why the PDCA model used in developing and maintaining an ISMS has been greeted with enthusiasm in those countries. However, legal frameworks were also identified as giving more central guidance than in typical Western cultures. More work needs to be done, however, to see why it may be advisable for PDCA to have legal reinforcement to be effective. The same PDCA principles are applied successfully to quality standards such as ISO9001 in Western cultures

Most recently, with different groups of co-workers, Sanchez (2009, 2010) has provided further useful insights into ISMS development in SMEs, which (like the Korean study) could inform future practice. The first of these studies (Sanchez et al, 2009) echoed previous studies about the differences between small business information systems and those of larger companies. The article noted that:

> "…in spite of the fact that there are still many enterprises assuming the risk of lacking adequate protection measures, there are many others that have understood that information systems are not useful without security management systems and the protection measures associated with them"
>
> (Sanchez et al, 2009, p.1)

and acknowledged previous research findings along similar lines from three years earlier (Doherty & Fulford, 2006) before the ISO27001 standard was launched.

4.2 Research conducted in the West Midlands

Local factors matter, as outlined in a recent report to the National Endowment for Science, Technology and the Arts (NESTA, 2010). The West Midlands has identified itself as falling behind other regions in terms of using information technology in business (AWM, The Digital Divide, 2007). There has consequently been quite a lot of recent activity (NB2BC, Business Link, Technology at Work, 2009) to try to encourage businesses to make more effective use of technology, and this is greatly welcomed by the authors of this report. There is little point in making investment in hardware and software unless investment is also made in utilising these with the digital information infrastructure to improve business processes.

Investment in information systems, however, should also mean at least some investment in information assurance. Recent research on SMEs in the West Midlands by the University of Worcester (Arthur, 2009) indicated that:

- Businesses had a general low awareness of information security controls and legislation
- Only 42% of organisations surveyed currently have an information security policy in place
- Only 6% of those who don't currently have a policy, have plans to introduce one
- Training in information security is viewed with average, or increasing importance amongst respondents
- 12% were currently interested in training or support with information risk management, and 23% would potentially be interested in the future
- There was a low awareness of potential funding available to assist small businesses

In common with the other on-line surveys on information security that have been reviewed here, one interesting phenomenon was the low response rate. No direct follow up research was done, but a number of factors would certainly have contributed to the response rate:

- getting the questionnaire to the right person i.e. an employee who is able to answer questions relating to information security

- whether "the right person" has (or is allowed/allows themselves) time to complete online questionnaire

- businesses are unlikely to want to even ask questions about a subject that may be controversial to them so there is little motivation to get it to the right person

If it is true that many businesses aren't quite sure who is responsible for information security - and the responses so far to our latest questionnaire (appendix 5) do suggest that this may indeed be so - this is itself a slightly worrying matter. If no-one is responsible, no-one is accountable (a basic information security principle). More detailed research has been, and continues to be conducted with West Midlands SMEs on an individual basis via interview to find answers to these more searching questions relating to information assurance. This research is ongoing, and continues to inform the development of the IASME model; results and analysis are not yet available.

As with the Sanchez et al SME study in Spain, the online West Midlands study conducted at Worcester highlighted the most likely reasons for the lack of a single point of responsibility as a lack of understanding and lack of support from senior management. Perhaps surprisingly, even in larger organisations the appointment of a person responsible at a senior level for the well-being of an organisation's information assets is a relatively recent phenomenon. Also, the appointment may be made at a middle-management grade and such a person may not have the standing of, say, the Marketing Director or Financial Director. Worse, the responsibility may fall to an existing Director who may have collected this responsibility along with other miscellaneous 'hats' and may have little or no experience in the subject. Even worse is the possibility that no-one at Board level is taking responsibility. Unfortunately, this subject is sometimes mistakenly not regarded as core business; research findings show that it is almost universally unsuccessful without Board level support.

The surveys also provide evidence from that the lack of an information security "supremo", results in information security responsibility being delegated to the IT department, who are unlikely to have the authority to make decisions affecting the conduct of the whole organisation. They may not have a voice at the Board, may have little or no budget for security, or may resent being given another impossible thing to do before breakfast, and so systematic information security can easily be overlooked. Such an approach may, therefore, be worse than useless to protect a business's information assets, as there may be a (misguided) warm feeling that the problem is under control, when in fact a number of potential threats could at any time become a data breach.

4.3 Recent Private Sector and Government-sponsored Research

Several high profile organisations have been producing research on many aspects of information security for many years, and the data gathered is useful for longitudinal studies seeking to establish trends. The amount of such research has increased dramatically in recent years, and the 2009 surveys have in many cases been just recently published. The most detailed and relevant of these are discussed in this section; as with academic research, a full list is available as an appendix (appendix 2).

In 2008, the then newly-formed government department of Business, Enterprise, and Regulatory Reform (BERR) produced an excellent "Data Breaches Survey" (BERR, 2008). BERR have now metamorphosed into BIS, but the important thing is that they published data on an annual basis. The data obtained in 2007 – the year the UK had its biggest ever loss of personal data - and comparison was made with data obtained five years earlier, in 2002. One conclusion of the 2008 report was that security was improving, but what this obscured was that the improvement was patchy and the threat was still growing.

PriceWaterhouseCoopers have been producing a detailed information security report annually for a number of years, asking some different, and some unchanged questions on each occasion. The 2010 survey uses data obtained in 2009, and comparison is made with figures for 2008. However, the focus is on larger, global organisations, which in itself doesn't tell much about the behaviour of SMEs. However, they do the confirm the trend that Henson and Hallas identified in their 2009 study which showed Asian companies powering ahead with ISO27001 certification, compared to the UK and most of Europe. One can only speculate about future prospects for global companies, but it seems unlikely that good information security will hinder a company's International reputation. The 2010 survey is entitled "Trial by Fire", alluding to the regulations and laws that are anticipated to come into force in the US in 2010; the only one of these that will directly affect UK organisations is the changes to PCI-DSS later this year (PCI, 2010). A detailed survey of current PCI-DSS attitudes in the UK (Bitpipe, 2010) shows remarkable complacency despite the stated intention of the credit card industry to impose considerable fines and even taking merchant services facilities away from organisations who experience serious breaches.

The Ponemon Institute have also been gathering thought-provoking data on matters relating to information security for a number of years, and these have been published by the PGP corporation. Of particular interest are the industry statistics they have been using since 2007 to work out the "per record" cost of a data breach in France, Germany, the US, and the UK. These have shown that the costs of recovery from a data breach are relentless rising, and whilst the data was obtained mostly from larger companies, there is no reason to think the costs would be significantly lower for SMEs. The quoted 2009 figures of, on average, £64 per record, up from £60 in 2008 (PGP, 2010) should focus minds doubtful about the value of information assets.

The Verizon Data Breaches report mentioned in the introduction (Verizon, 2009a) is in many respects excellent, but unfortunately the breakdown of businesses into sizes is not along conventional SME lines, and unfortunately the data is not closely analysed. It does, however, show an interesting double-peak graph of breaches/company size, and the middle trough occurs within organisations of 100-1000, only some of which (100-250) are SMEs. A more detailed study of organisations and data breaches according to size/nature of business would perhaps give some insight into why the trough/twin peaks have occurred, and what lessons could be learned by other businesses. Verizon also produced a fascination supplementary report "Anatomy of a Data Breach" (Verizon, 2009b) which explores and identifies typical exploited vulnerabilities in greater depth. However, Verizon is a US-based company where SME becomes SMB, and in any case the definitions do not follow EU guidelines.

Figures obtained so far for 2010 show that the number of breaches reported continues to increase. Figures for the UK are still hard to come by, but figures released so far in the US, as reported to the Identity Theft website (ITRC, 2010), show 325 breaches already this year involving a total of 8,320,325 records. This compares to 498 breaches for the whole of 2009 (ITRC, 2009). The nearest equivalent UK repository can be found on the ICO website, but “naming and shaming” only happens in the most serious cases, and data is only released sporadically through “press releases from the ICO”, which have already been identified in this report as being not as up-to-date as they were before the 2010 election, and one hopes this is only a temporary matter.

The latest figures from a worldwide study on SME spending on information security, compared to the average cost of a data breach (Symantec, 2010) give some encouragement. However, there is some concern amongst security professionals that this view of company economics is giving SMEs the (false) message that it is worthwhile taking the risk and just setting aside the money as preparation for that breach.

5. Internal and External Threats, Vulnerabilities, and The Changing Threat Landscape

Like CIA (confidentiality, integrity and availability), these are familiar terms to information security professionals, but not to a wider audience. However, the basic principles can be easily explained to SMEs, in terms that may prompt them to take the necessary action.

5.1 Threats

These can be conveniently categorised as “internal” and “external”.

Internal threats often come from employees, and incidents are typified in appendix 3. What happens within an organisation is not part of national infrastructure, but can, through its collaboration partners, have a big impact on the protection of data transported nationally, and indeed internationally.

External threats include anyone trying to gain access to an organisation’s data, as explained in appendix 4. For the SMEs that are connected to the Internet, this means a huge, and growing, number of people.

5.2 Vulnerabilities

Vulnerabilities provide a means of attacking information assets. Those who harm information assets do so through (accidentally or on purpose) exploiting them. Controlling potential vulnerabilities to protect information assets is what information security is all about. However, exercising this control is a potentially expensive business in itself, which needs to be managed.

Economics of Information Security academics have created elaborate mathematical models to inform businesses when to stop spending on plugging vulnerabilities because of an ever diminishing return. A system can never be completely secure, but up to the point where the spend vs. protection relationship tails off, more money appropriately targeted will generally bring greater security.

5.3 Research on Threats: Insider Greatest?

One reason that information security is so hard is that the potential threats are constantly changing. For example, it wasn't until 2005 that the scale of the insider threat was properly quantified (Deloitte Touche, 2005), and identified as being – at that time, at least - the greatest threat of all, in terms of incidents reported.

Within larger organizations, this realization brought about an increasing focus on the actions of disaffected or careless employees, and brought about a new academic area of study: "Human Factors in Information Security". The support given to public sector organizations as a result of the 26.7 million record loss by HMRC (Her Majesty's Revenue and Customs) particularly focused on having information security procedures in place, and making sure employees are educated about the use of such procedures so that insiders will be less of a threat to organisational data. The work that has been recently done in larger organizations, particular the UK public sector, to combat the insider threat was an acknowledgement of its importance.

However, surveys conducted with SMEs before and after the HMRC incident indicate that documenting and implementing procedures relating to IT has never been a strong feature of SME behaviour. The insider threat consequently received a lot of publicity in the media as the 2008-9 recession caused a lot of people to be concerned about their jobs. Some developments will have recently taken place within UK SMEs to combat the insider threat as a result of increasing awareness, but without the funding and management structure to impose this from above (as is the case with public sector), in many SMEs the insider threat will still be very real.

5.4 External Threats via "Cyber attacks" now causing more damage than Insiders

The threats from outside, however, are continuing to increase. The very latest research shows that outsider threats are actually growing at an alarming pace. One study () shows that external interference is now causing even more incidents than the activities of insiders. In this digital world, "outside" usually means The internet. As more people use this world wide network, and use it in ever more sophisticated ways, it can be expected that threats from outside will increase.

The UK's Centre for Protection of National Infrastructure (CPNI) lists information security as one of its areas of influence, and considers that government and innovative businesses remain under threat from espionage, and monitored external threats closely. The threat of electronic attacks, in particular malware, hacking, botnets, keystroke logging and denial of service, is explained on the CPNI website (CPNI, 2010). It is worthy of ironical note that in spite of all the physical protection methods for citizens at International airports, USB-based keystroke logging devices are currently commercially available in airport shops.

The threat from espionage (spying) did not end with the collapse of Soviet communism in the early 1990s. Espionage against UK interests continues from many quarters.

In the past, espionage activity was typically directed towards obtaining political and military intelligence. This remains the case, but in today's high-tech world, the intelligence requirements of a number of countries also include new communications technologies, IT, genetics, aviation, lasers, optics, electronics and many other fields.

The UK is a high priority espionage target and a number of countries are actively seeking UK information and material to advance their own military, technological, political and economic interests.

The threat against UK interests is not confined to the UK itself. A foreign intelligence service operates best in its own country and some may therefore find it easier to target UK interests at home, where they can control the environment and where the UK traveller may let their guard drop. In mid-2009 PriceWaterhouseCoopers produced a report on what it called ‘E-espionage’, looking at the threat to business information confidentiality, integrity and availability from outside the organisation. The report considers that

“Today, the risk of espionage is current and concrete for all organisations worldwide, across both the private and public sectors. A major driver behind this threat is the growing reliance on internet-enabled computer systems for storing, processing and communicating business-critical digital information across organisational boundaries, and the increase of telecommunications across the Internet.

These trends have given rise to a new and specific term for the risk that confidential information may be compromised or stolen by external criminals: ‘E-espionage’.

“Every minute of every day, a growing number of well-resourced and highly sophisticated cyber-criminals from across the world are seeking to gain unauthorised access to valuable data held by companies and governments. And the increasingly interconnected and open nature of today’s internet-enabled corporate systems is helping to boost their opportunities.”

(PWC, 2008, p.)

“Large organizations are by now well aware of these threats, and their reported security incidents are falling. However, evidence from smaller

organizations suggests that numbers of incidents are rising, perhaps suggesting that the external threat is now turning onto them."
(Ponemon Institute, 2010)

This is reassuring for large organisations, and the extra safeguards should make sure they have sufficient protection against such threats. However, the SME may not even be aware of the need to have a system in place to counteract such threats, which will make them an obvious "weak link" target.

6. Possible Consequences of SME inaction

This is not just about plugging holes in vulnerabilities and creating policy and procedures for employees. Information assurance is actually a more tactical and strategic matter. An interesting paper (Nemertes Research, 2008) postulates that the business that regards improved information security (i.e. better awareness of threats and control of vulnerabilities) as generating a return on risk can take market opportunities others cannot. For example, there are two main consequences for the business as far as a typical information assurance decision is concerned:

- the business takes too little risk and fails to take advantage of opportunities through fear and ignorance. Wiser competitors may take that market advantage.

- The business takes too much risk with its information assets and inevitably bites the dust through losing or mishandling its data. Cash flow, reputation and loss of lead over competitors can result.

The most recent annual study carried out by the Ponemon Institute, based on 33 institutions in 10 different UK industry sectors, indicates that:

"UK industry continues to suffer very expensive data breaches – the average cost of a breach was £1.68m, the most expensive being nearly £3.9m. The average cost per record rose slightly to £64. This was despite the perception that a data breach did not grab the headlines as it used to.

- Data breaches arising from malware had doubled from 2008 and cost substantially more than human causes or IT glitches. The risk of damage or loss of information from the outside of an organisation is now higher than from the insider.

- Thirty-six percent of breaches involved outsourced third party facilities, which were considerably more expensive per record than in-house (£81 vs. £55), probably due to higher forensic investigations and consulting fees.

- While public sector organisations costs per breach were similar to the private sector, the public sector spent considerably more on detection,

> response and notification. This was probably due to the increased government attention to improving these areas.
>
> (Ponemon Institute, 2010)

A similar pattern is presented by Sophos in their Data Breaches report covering incidents occurring in 2009 (Sophos, 2010). Private sector costs through loss of business were 87 percent higher than the public sector and remains the most significant consequence of data breaches. Other surveys present a similar picture. The threat is real, and it continues to grow. If an SME does not heed these warnings and fails to allocate sufficient resources to information security, they are unlikely to have confidence in information assurance processes. Information risks may not be contemplated, and market opportunities could be missed.

It can be concluded that the potential business danger to SMEs is indeed a very real one. However, the risk does not stop there, because (as already mentioned) there is also a legal liability, which is gradually being tightened. Apart from the Data Protection Act, a number of other UK laws relate to organisations information assets, including:

Computer Misuse Act 1990
PCI DSS (credit card data)
Electronic Communications Act 2000
Regulation of Investigatory Powers Act 2000
Laws Pertaining to Financial Data

It would be interesting to speculate whether private sector spending on protecting their data does increase as a result of the new penalties for data protection infringements (i.e. fines up to £500000) introduced on 6 April 2010.

7 THE IASME Consortium

7.1 Role in Supporting SMEs

IASME is an Information Infrastructure project to provide support and guidance leading to affordable information assurance for SMEs.

It acknowledges that local and regional factors are of significance to SMEs, and therefore chooses to focus on a particular region which is well-known to the project team: the West Midlands. It also acknowledges that every small business is unique and exists to support SMEs in providing and implementing information security procedures that are appropriate for their own needs. This means that the IASME role is an ambitious one that goes way beyond the conventional university model of providing bespoke courses to a range of businesses with the expectation that there will be knowledge of sufficient use to all attendees to justify the cost of the course. However, this is a model that has previously failed due to an acknowledgement of the unique needs of individual businesses and the consequent need for one-one knowledge transfer.

7.2 SMES and ISO27001

The ISO27001 standard is widely regarded as the best way for larger organizations to safeguard their information assets. A full scale ISMS (information Security Management System) following the spirit if not the compliance requirements for ISO27001 may indeed be perceived as being the minimum required also to satisfy an SME's needs. However, this is not inevitably the case and each SME deserves to be considered on its own merits.

The limited resources of smaller companies mean that they are often unable to focus as closely as they may wish on what may be perceived as peripheral activities, including information security. Also, the lack of action is not just a problem for the SMEs themselves. The recent University of Worcester survey merely reinforced research all the earlier academic and private sector research previously conducted elsewhere, building on an existing concern that security vulnerability in one link can create vulnerability right across the supply chain. Focused attacks on the nation's information infrastructure may already be moving from larger companies with dedicated resources for protection to poorly defended SMEs who provide quicker wins.

7.3 SMEs and ISMS Development

Development of an ISMS (information security management system) and certification to the International standard ISO/IEC 27001 is the accepted good practice and provides the best information assurance for any organization. However, it is time-consuming, expensive, and hard to scale to the SME business model. The IASME project intends to address these major problems by identifying an intermediate level of information security controls and developing entry-level certification for SMEs whilst encouraging working towards full compliance with the International standard where the opportunity arises.

The accredited certification process will initially be offered through the NCC (National Computing Centre) and a mark of excellence will be developed for use in letterheads and publicity to demonstrate the level of assurance attained by the organization.

8 Conclusions

8.1 Prospects for full-blown ISO27001

The University of Worcester 2009 survey reinforced the evidence that most SMEs have not given enough attention to information security, but also showed that, despite all the high profile incidents and horror stories of data breaches most SMEs still had no plans to introduce systematic information security. The recession was considered to be a significant factor here, with the risk of staying in business seen as more important than safeguarding information security processes.

The general perception was that this was an understandable reaction, However, the huge amount of research data that has been accumulating since 2001 suggests that the costs of an information security breach can be immense, and indeed sufficient on their own to put a small business out of business. Justification in terms of "staying in business" didn't make the problem go away, and won't reduce the costs to an SME of an information breach.

Those organisations that are now in a position to do so should therefore be at least aspiring towards ISO27001 compliance or even full certification to give them the satisfaction that they are protecting their precious information assets to the highest available standard. However, such organisations will need highly specialised knowledge transfer sessions over an extended period to successfully achieve ISO27001, which will be expensive. There is also scope to provide organisations possessing more limited resources with an ongoing support for and acknowledgement of their efforts towards developing an ISMS, and that is where the IASME approach to knowledge transfer has a clear role.

8.2 Prospects for adoption on a "Maturity Model"

Apart from the issues of responsibility, accountability, and management of information assurance that have already been discussed, the message we were getting from questionnaires and interviews with senior managers of SMEs was that:

1. they were very reluctant to put resources into securing their information during the recession

2. many at least acknowledged that the problem would not go away, and it would need attention at some stage in the future

It was therefore considered that, as the effects of this recession started to subside, the matter of safeguarding information assets might become more of a priority for SMEs, but that few would be thinking in terms of achieving the highest available standard. Hence, there was a very clear need for an intermediate product that would allow meaningful and worthwhile development to occur in stages, and an maturity model would seem a sensible way for the small business to "grow" their ISMS. The IASME model intends to produce an information assurance product aimed at SMEs with this purpose in mind.

8.3 Summary

Research indicates that:

- The threat of loss of confidentiality, integrity and availability of business information is real and increasing.

- The consequences of information loss can be very expensive in terms of cost, reputation and legal action.

- SMEs in the West Midlands seem to be ill prepared to meet this threat

The IASME scheme is intended to be a cost-effective way to help SMEs understand their level of preparedness and to help them to improve.

The IASME model has been tested with a series of interested organisations that have agreed to act as pilots. The purpose of this final stage was to ensure that the model really does meet the unique needs of small businesses, and feedback has informed fine tuning for a roll out of the IASME product and service across the West Midlands from the end of 2010.

9 References

Adroit Economics, 2007, "West Midlands high impact ICT Strategy",
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.
Anderson R, 2002, "Maybe we spend too much", Inaugural meeting of WEIS, Berkeley, California
Anderson, R., 2009, "WEIS 2009 Live Blog", http://www.lightbluetouchpaper.org/2009/06/24/weis-2009-liveblog [accessed 25th June 2010]
Arthur J, 2009, "Information Security survey of SMEs for Worcester Business School"
Backhouse J, Hsu CW, Silva L, 2006, "… de jure standards: shaping an international information systems security …", Management Information Systems, 2006
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.
BERR, 2008. "*2008 Information Security Breaches Survey",* Department for Business, Enterprise & Regulatory Reform, http://www.berr.gov.uk/files/file45714.pdf (accessed 27/07/09)
BERR, 2009, "Enterprise Directorate: Small and Medium Enterprise Statistics for the UK and Regions", Department for Business, Enterprise & Regulatory Reform, http://stats.berr.gov.uk/ed/sme/smestats2008-ukspr.pdf (accessed 19/04/10)
Clear, F, 2007, SMEs, electronically-mediated working and data security: cause for concern?
Coles-Kemp, E., & Overill R., 2007, "The design of Information Systems for small-and-medium sized enterprises" in, Remenyi D (ed), "Proceedings of the 6th European Conference on Information Warfare & Security".
Computer Weekly, 2010, "Data Protection Act is out of kilter with EU law, warns privacy lawyer" http://www.computerweekly.com/Articles/2010/06/09/241513/Data-Protection-Act-is-out-of-kilter-with-EU-law-warns-privacy.htm [accessed 5th July 2010]
CPNI, 2010, "Electronic Attacks". Accessed from http://www.cpni.gov.uk/MethodsOfAttack/electronic.aspx
Dimopoulos V, Furnell S, Jennex M, Kritharas I, 2004, "Approaches to IT Security in Small and Medium Enterprises" in "Securing the Future: 2nd Australian Information Security Management Conference".
Doherty, N. F. and H. Fulford (2006)] Doherty, N. F. and H. Fulford: "Aligning the Information Security Policy with the Strategic Information Systems Plan." *Computers & Security* (2006), 25(2): 55-63.
Dojkovski, S, Lichtenstein, S and Warren, M 2007, "Fostering information security culture in small and medium size enterprises: an interpretive study in Australia"*, in Proceedings of the 15th European Conference on Information Systems*, University of St. Gallen, St. Gallen, Switzerland, pp. 1560-1571.
Ernst & Young, 2008, "Moving Beyond Compliance: Ernst & Young 2008 Global Information Security Survey", p.6.

EU, 2005, "The New SME Definition: user guide and model declaration" http://ec.europa.eu/enterprise/policies/sme/files/sme_definition/sme_user_guide_en.pdf [accessed 5th July 2010]
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.
HMG, 2010, National CyberSecurity Strategy HMSO
IASME, 2010, "IASME - Information Assurance for SME", http://iasme.ncc.co.uk [accessed 5th July 2010]
ICO, 2004, "Data Protection and Small and Medium Enterprises", http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/dataprotectioninsmes.pdf [accessed 5th July 2010]
ICO, 2007, Report on SMEs, summarized in http://www.business-inc.co.uk/news/2007/october/smes-failing-to.htm
ICO, 2010a, "Data Protection and Freedom of Information Advice" http://www.ico.gov.uk [accessed 5th July 2010]
ICO, 2010b, "Statement: European data protection Commission's call for the UK to strengthen the powers of its national data protection authority" http://www.ico.gov.uk/upload/documents/pressreleases/2010/ico_statement_european_commission_280610.pdf [accessed 5th July 2010]
ITRC, 2010, "ITRC Breach Report 2010", http://www.idtheftcenter.org/ITRC%20Breach%20Report%202010.pdf [accessed 23rd June 2010]
ITRC, 2009, "ITRC Breach Report 2009", http://www.idtheftcenter.org/ITRC%20Breach%20Report%202009.pdf [accessed 23rd June 2009]
Kluge D, and Sambasivam S, 2008, "Formal Information Security Standards in German Medium Enterprises", CONISAR 2008.
Lee W-S, and Jang S-S, 2009, "A Study on Information Security Management System Model for Small and Medium Enterprises
Levy M, Powell P, and Yetton P, 2002, "The Dynamics of SME Information Systems", Small Business Economics, Volume 19, Number 4 / December, 2002, pp. 341-354.
Nemertes Research, 2008, "Not an End In Itself: Information Protection and Return on Risk"
NESTA, 2010, "Local Knowledge: Case Studies of four innovative places", http://www.nesta.org.uk/library/documents/Local-Knowledge-130410.pdf [accessed 5th July 2010]
Price-Waterhouse-Coopers, 2008, "Safeguarding the new currency of Business", p.2.
Price-Waterhouse-Coopers, 2008, "E-espionage: What risks does your organisation face from cyber-attacks", July 2008.
Price-Waterhouse-Coopers, 2010, "Trial by Fire", March 2010 http://www.pwc.com/en_GX/gx/information-security-survey/pdf/pwcsurvey2010_report.pdf
PGP Corporation, 2010, "2009 Annual Study: UK Cost of a Data Breach"
Sánchez L E, Parra A S-O, Rosado D G, Piattini M, "Managing Security and its Maturity in Small and Medium-sized Enterprises", *Journal of Universal Computer Science, vol. 15, no. 15 (2009), 3038-3058*

Sánchez L E, Ruiz C, Fernández-Medina E, Piattini M., “Managing the Asset Risk of SMEs”**,** 2010 International Conference on Availability, Reliability and Security, pp. 422-429

http://www.computer.org/portal/web/csdl/doi/10.1109/ARES.2010.52

Schneier B., 2002, “No, we don’t spend enough”, Inaugural meeting of WEIS, Berkeley, California

Symantec, 2010, “Symantic 2010 SMB Data protection Survey”, http://www.symantec.com/content/en/us/about/media/pdfs/SMB_ProtectionSurvey_2010.pdf [accessed 25th June 2010]

Verizon 2008, “2008 Data Breach Investigations Report”, Verizon Business

Verizon, 2009a, “2009 Data Breach Investigations Report”, Verizon Business

Verizon, 2009b, “2009 Data Breach Investigations Supplementary Report: Anatomy of a Breach”, Verizon Business

Appendix 1 – List of Academic Studies

Arthur J, 2009, "Information Security survey of SMEs for Worcester Business School"
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.
Coles-Kemp, E., & Overill R., 2007, "The design of Information Systems for small-and-medium sized enterprises" in, Remenyi D (ed), "Proceedings of the 6th European Conference on Information Warfare & Security".
Dojkovski, S, Lichtenstein, S and Warren, M 2007, "Fostering information security culture in small and medium size enterprises: an interpretive study in Australia"*, in Proceedings of the 15th European Conference on Information Systems*, University of St. Gallen, St. Gallen, Switzerland, pp. 1560-1571.
Faisal M N, Banwet D K, & Shankar S, 2007, "Supply chain risk management in SMEs: analysing the barriers", *International Journal of Management and Enterprise Development (IJMED), Vol. 4, No. 5, 2007*
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.
ICO, 2004, "Data Protection and Small and Medium Enterprises", http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/dataprotectioninsmes.pdf [accessed 5th July 2010]
ICO, 2007, Report on SMEs, summarized in http://www.business-inc.co.uk/news/2007/october/smes-failing-to.htm
Kluge D, and Sambasivam S, 2008, "Formal Information Security Standards in German Medium Enterprises", CONISAR 2008.
Sánchez L E, Parra A S-O, Rosado D G, Piattini M, "Managing Security and its Maturity in Small and Medium-sized Enterprises", *Journal of Universal Computer Science, vol. 15, no. 15 (2009), 3038-3058*

Sánchez L E, Ruiz C, Fernández-Medina E, Piattini M., "Managing the Asset Risk of SMEs", 2010 International Conference on Availability, Reliability and Security, pp. 422-429

Appendix 2 – Recent Private Sector/Government Studies

BERR, 2008. "*2008 Information Security Breaches Survey",* Department for Business, Enterprise & Regulatory Reform.
BERR, 2009, "Enterprise Directorate: Small and Medium Enterprise Statistics for the UK and Regions", Department for Business, Enterprise & Regulatory Reform.
Ernst & Young, 2008, "Moving Beyond Compliance: Ernst & Young 2008 Global Information Security Survey".
ITRC, 2010, "ITRC Breach Report 2010“, http://www.idtheftcenter.org/ITRC%20Breach%20Report%202010.pdf [accessed 23rd June 2010]
ITRC, 2009, "ITRC Breach Report 2009",

http://www.idtheftcenter.org/ITRC%20Breach%20Report%202009.pdf
Nemertes Research, 2008, “Not an End In Itself: Information Protection and Return on Risk”
Price-Waterhouse-Coopers, 2008, “Safeguarding the new currency of Business”.
Price-Waterhouse-Coopers, 2008, “E-espionage: What risks does your organisation face from cyber-attacks”, July 2008.
PGP Corporation, 2010, “2009 Annual Study: UK Cost of a Data Breach”
Symantec, 2010, “Symantic 2010 SMB Data protection Survey”, http://www.symantec.com/content/en/us/about/media/pdfs/SMB_ProtectionSurvey_2010.pdf [accessed 25th June 2010]
Tripwire, 2010, “PCI Compliance: Are UK Businesses Ready?”, Tripwire.
Verizon 2008, “2008 Data Breach Investigations Report”, Verizon Business
Verizon, 2009a, “2009 Data Breach Investigations Report”, Verizon Business
Verizon, 2009b, “2009 Data Breach Investigations Supplementary Report: Anatomy of a Breach”, Verizon Business

Appendix 3 – Possible Threats to Digital Information held by SMEs from Insiders

Typical sources of threat might include:

- hard-working and otherwise dedicated employees accidentally misusing data due to ignorance or carelessness
- disaffected, careless or dishonest employees wishing to cause harm to the organization

Both can have devastating effects. This is a matter that can only be addressed with administrative assistance from management.

Appendix 4: Information Security Threats from Outside the Organisation

These include:

Amateur or professional hackers;
Virus and other malware;
Visitors, including Investigative journalists;
Commercial competitors (i.e. industrial espionage);
Political pressure groups/activists;
Organised criminal groups;
Physical threats, including disaster and terrorist activity.

All organisations will be threatened by one or more of these sources; to ignore this fact is to put a business at risk. External interference has always been a very real threat for organizations connected to the Internet.

Management involvement again needed – e.g. employees can inadvertently download viruses unless procedures are in place to prevent that happening, and they are aware of those procedures.