SMEs, Information Risk Management, and ROI

Richard Henson, University of Worcester
Bruce Hallas, Marmalade Box Consulting

Abstract

Recent research in the area of standards accreditation has shown that the rate of take up of the ISO27001 (Information Security Management) by organisations been disappointing in many Western countries, compared to the picture emerging in Asia, and the rollout of previous international standards that relate to information management, such as ISO9001.

In this paper, a researcher and a practitioner from the UK investigate possible reasons for a lesser interest in pursuing certification for organisational Information Security Management Systems (ISMS) across Western countries. They also share their perceptions and concerns that current attitudes of UK of small businesses regarding complying with standards and legislation means that they may be taking unnecessary risks with their corporate and personal data under the possibly misguided notion that other priorities are more important during these current recessionary times.

The authors use an economics-based approach in proposing a solution to the problem. On the one hand they review the research that has provided methods for putting a figure on the value of corporate and personal data in larger organisations, and applying the principles of managing information risk as appropriate to SMEs. On the other hand they look at economics-related issues such as market pressure, insurance, outsourcing, and the legal and regulatory matters regarding privacy of personal data. The result provides a case for showing SMEs that, apart from the moral matter of being “good for the business”, there are very sound economic reasons for an SME developing an ISMS and getting ISO27001 certified.

SME, Information Risk Management, ISMS, Information Security Management Systems, Data Protection Legislation, Economics of Information Security, Value of Data, ISO27001, PCI DSS, Drivers for Accreditation

Introduction

"Information is the new currency of business - a critical corporate asset whose value rises and falls at different times, and in different ways, depending on when, how, where and by whom it is placed into circulation as a medium of exchange. Therein lie the risks. And the opportunities."
(PriceWaterhouseCoopers, 2008, p.1)

So large organizations may be recognizing that the world of doing business has changed, that good management of their digital information is a key factor to success. However, the extent to which this message is filtering through to SMEs (Small and Medium Sized Enterprises) is not well researched. This paper will look comparatively at how widely the Information Security Management System (ISMS) model is being adopted across Europe and globally. It also looks at recent trends in the UK and elsewhere in view of the recession and takes a preliminary view of the drivers for robust organizational ISMS, and how they might, or might not, influence SMEs.

The drivers for organisations to develop an ISMS and get it certified

"Economics of Information Security" was initiated by a debate on organisational spending on security (Anderson, 2002; Schneier, 2002), to investigate economic factors driving the development of organisational ISMSs. Subsequently, researchers have identified a number of issues that organizations need to look out for when consider whether or not to spend more on Information Security, and can be considered as drivers towards compliance and certification to the ISO27001 standard. An alternative research approach to ISMS development is "Human Factors in Information Security", and this has grown in parallel.

The first thing to note about organisational ISMS development is that it can be an expensive undertaking, which needs financial justification. The authors of this paper would wish that organizations would recognize the main driver towards an ISMS as "because it is good for the business". Maybe one day that will be the case, but all business costs need to be justified, and that includes ISMS development. It therefore makes sense in the interim to use an economics approach, and find reasons to develop an ISMS that contributes towards profitability..

As Bartlette & Fomin (2008) discovered, surprisingly little Economics of Information Security research to date has focussed on ISMS certification or how economics may particularly impinge on the unique environment of an SME. In their fascinating paper, they briefly considered factors that might explain the low ISO27001 accreditation rates within organisations, and the apparent anomaly compared to what could be perceived as a rush for compliance with other international standards such as ISO9001. However, when seeking explanations in their subsequent paper, they mainly identified possible "human factor" drivers (or barriers) and acknowledged that more research was urgently needed.

As the current paper focuses on SMEs, it will seek explanations in terms of the economic motivators that have been identified by researchers as influencing organisational decision-making. These are listed below, will be considered in turn:

I. Legal and Regulatory (avoiding fines; retaining right to trade)
II. Protection of Reputation & Brand (reputation damage; lose market share)
III. Market Pressure (risk of loss of customers)
IV. Physical Cost of a Data Breach
V. Loss in stock market value if a breach is publicized
VI. Insurance premiums (higher as a result of data breach)
VII Outsourcing (possibly increased chance of a data breach)

Measuring ISMS activity

We could have adopted two possible approaches, and both are considered here.

1. We could choose information security policy as the measure

This is a measure popularly used by information security surveys (positive outcome = the policy document). A number of options are already available for gathering data about organisations and information security policies. Firstly, many statistics are provided by government-based organisations such as BERR in the UK (BERR, 2008), or other national statistics. One problem here was that the questions asked in the surveys didn't seem to be quite the same, making direct comparison difficult. The worldwide surveys by Ernst and Young (2008) and the more independent Ponemon Institute (PGP, 2009) seemed more useful because the same questions were being asked in different countries.

2. We could use choosing an ISMS as the measure

An ISMS is an implementation of a model for managing information security within an organisation. This is a complex matter, and every organisation is unique. Over the last twenty years or so, a tremendous amount of work and expertise has gone into developing a number of different, or related, models for managing an organisation's information systems. Ever more elaborate and sophisticated models emerged to reflect different types of organisations and different complexities of networks and internetworks. Just choosing, or "registering" an ISMS = positive outcome. However, according to a recent researcher this would be far from a useful measure…

"… registering an ISMS still says nothing about the quality and performance of its implementation. Therefore, in this article, a method for measuring the performance of the implementation and operation of an ISMS is presented" (Boehmer, 2008, abstract)

3. We could choose ISMS accreditation as the measure

This approach has been avoided in the global surveys. (different models became popular in different countries; standards often used for benchmarking but a decision made not to become certified; no universally accepted measure)

However, as time has moved on, thankfully there has been a convergence of opinion amongst researchers and practitioners as regards what constitutes a robust ISMS and the various stages necessary for an organisation to acquire that robustness. The achievement of that robustness and effectiveness was rewarded by accreditation by one of a number of bodies such as ISACA, BSI (UK), BIAS (Germany), ISO, etc…

One possible way to obtain meaningful data for a country with so many organisations awarding information security management accreditation would be to sum up the outputs from a number of different certifications bodies. However, this would have been highly time-consuming and didn't really combine like with like. Also, which of the certifications on offer really met up to the definition of a standard? As the computer networks guru Andrew Tanenbaum cynically told us in his textbook "Computer Networks":

''The nice thing about standards is that there are so many to choose from. And if you really don't like all the standards you just have to wait another year until the one arises you are looking for.''

(Tanenbaum, 1988, p. 254)

We didn't have the luxury of waiting that extra year, so we looked closely at currently available standards (rather than methodologies) for an ISMS. **T**he most popular candidates were COBIT and ISO27001. Which to choose? Thankfully, other researchers before us have stated that:

"The Control Objectives for Information and Related Technology (COBIT) as well as the IT Infrastructure Library (ITIL) are often mentioned in connection with IT

security. Though the outcome of their implementation supports a company in establishing secure information systems, their main content deals with different matters, hence they have not been counted as IS standards..."

(Kluge & Sambasivam, 2008, p.2)

"… All other before mentioned standards including ITIL and COBIT and Grundschutz refer to ISO 27001 when it comes to certification (Szakats 2004; ISACA 2007; FOIS 2004)." (Kluge & Sambasivam, 2008, p.3)

This left little doubt that, if we were to use ISMS accreditation as our measure, ISO27001 certification would the most suitable single measure to use.

Choice of Methodology

Choice 2 seemed totally inappropriate because the data didn't give any indication about operational level.

This would probably also be the case for choice 1, but at least the matter of base level engagement/non-engagement was a potentially worthwhile measure. One disadvantage of using this measure would be that any research we carried out using other surveys would be secondary and would not necessarily provide a helpful picture for country-by-country comparison. Although detailed and interesting, these surveys also only provided a snapshot of the situation at a point in time, annually or biannually, which wouldn't be so useful for purposes of comparison and recent trends. Furthermore, we had our concerns about the validity of such data, for our purposes.

Recent survey results are held by their authors to be encouraging, showing a progressive increase in the percentage of organisations having devised a written information security policy. However, the focus is the existence of a policy document, and that measure gives no indication as to how that policy is effectively being implemented. Studies elsewhere in Europe (e.g. Kluge and Sambasivam, 2008) and anecdotal evidence obtained from businesses locally in the UK has suggested that an organisation merely saying on an online survey that they have an information security policy doesn't actually amount to very much on its own, and a yes/no response may present a more optimistic picture of developments towards an ISMS than is actually the case. We deduced that this type information security survey would be fine for capturing qualitative data, but would not be most appropriate for our current investigations.

Choice 3 was attractive partly because it was quantitative and we had ready access to the raw data, already categorised as country-by-country (ISMS, 2009). Provided that the data was "picked" at suitable time intervals we could make direct month-by-month comparisons.

We finally agreed that the best focus would be to choose the relevant ISO standard for ISMS, ISO27001. The actual measure used in our analysis would be the numbers of ISO27001 certificates awarded monthly, in each country, as the effects of the recession began to be felt by organisations and their workforces. Also, we felt, an output measured against an exacting standard is a much more meaningful benchmark than the existence of an unaudited document. Firstly because it actually means something in operating terms, and secondly because evidence of operational success of the output must also be available to the scrutiny of external audit before an ISO27001 certificate is awarded.

Data Used in the survey

The figures for ISMS being used in this study reflect the time from which the recession properly started and the end of June 2009. As the effects of the recession are

only just being fully realised, it would not be wise to make speculative projections about future trends for ISO certification based on future projections of economic growth. They are interesting not just longitudinally, for the trends over time in a particular country, but also horizontally for the wide discrepancies across different countries.

The total US figure may be not be an accurate reflection, because larger numbers of companies have used non-ISO27001 series bodies to accredit a robust ISMS. However, the trend in that country is still worth noting.

For the rest of the world ISO27001 does seem to be the favoured option, and the differences between developed countries are very marked. Two aspects of the data worth noting are:

(i) differences in numbers of certificates awarded within the 27 states that currently make up the EU.

(ii) higher levels of accreditation in many East Asian countries compared with elsewhere in the world

(i) Differences within Europe

To demonstrate (i), we chose ISO certification figures awarded within that country for twelve fairly representative European countries up to June 2009. We could have chosen a different month, but scrutiny of the data for other months showed that the differences would have been similar. Results are shown below (table 1):

Country	Total no. of ISO27001 certificates
Austria	30
Czech Republic	82
France	12
Germany	120
Greece	22
Hungary	65
Ireland	29
Italy	56
Poland	40
Slovakia	7
Spain	36
UK	402

Table 1: ISO27001 data for some European Countries taken at the end of June 2009

As can be clearly seen, the UK has a much higher figure than any other state. By contrast, certain of the smaller Eastern European states have absolute figures greater than large states such as France or Italy. If population is also taken into consideration, so that figure for each country is certificates per capita, the “Eastern Europe” and “English-speaking” effects are even more marked (table 2, table 3, graph 1, graph 2):

"Mature" EU countries

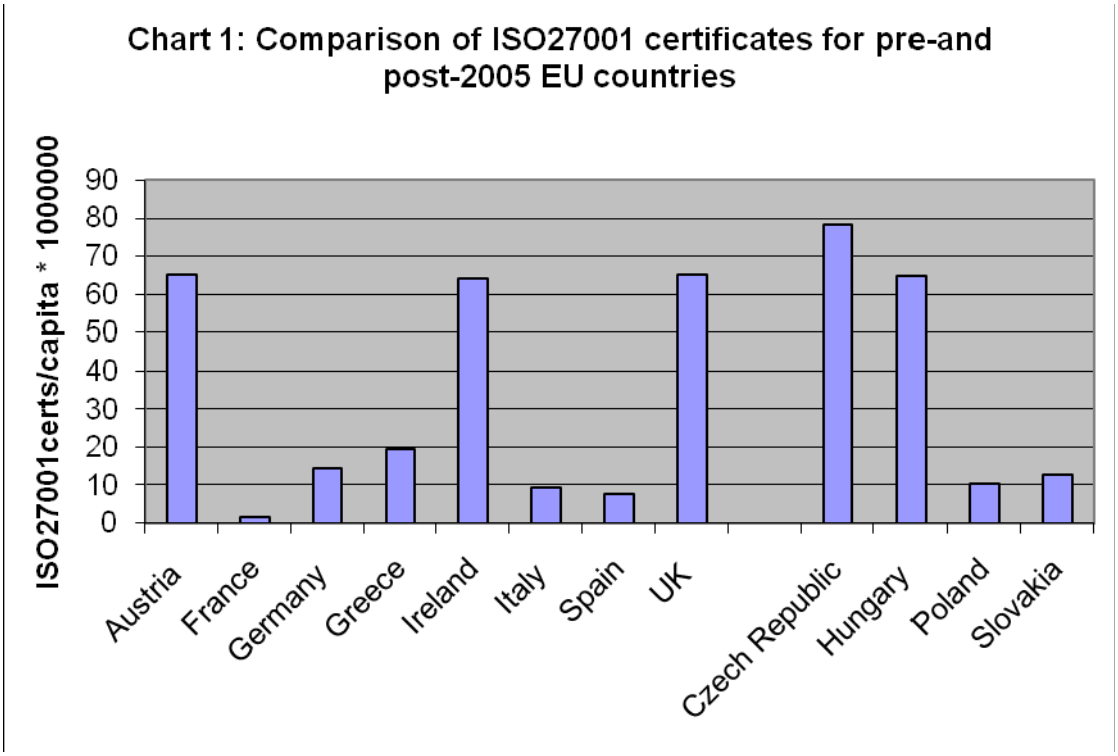
Country	Total no. of ISO27001 certificates	ISO27001 certificates per capita
Austria	30	0.0000649
France	12	0.0000018
Germany	120	0.0000146
Greece	22	0.0000195
Ireland	29	0.0000642
Italy	56	0.0000093
Spain	36	0.0000079
UK	402	0.0000652

Table 2: ISO27001 data per capita for pre-2005 European Countries taken at the end of June 2009

New EU Countries

Country	Total no. of ISO27001 certificates	ISO27001 certificates per capita
Czech Republic	82	0.0000783
Hungary	65	0.0000648
Poland	40	0.0000105
Slovakia	7	0.0000129

Table 3: ISO27001 data per capita for post-2005 European Countries taken at the end of June 2009



The above figures show a per capita difference of over 40x between the best performing country (Czech Republic) and the worst country (France) in terms of ISO27001 certificates awarded.

Some interesting possible trends are emerging here. Firstly, English-speaking countries seem to have much higher levels of ISMS per capita than the average for the EU. Secondly, a cluster of countries in central Europe (Austria, Czech Republic, Hungary) also seem to have much higher levels ISO27001 certificates per capita than might be expected.

The authors of this paper contend that ISO27001 is considered to be the best ISMS standard available, that organisations should be encouraged to strive towards this standard. In our opinion, many EU countries are falling well behind the best practice, and those doing well should be encouraged to share good practice with those who are below the average. Perhaps this is a matter that may be of interest to ENISA (European Network and Information Security Agency).

(ii) Statistics for ISO27001 take up globally

It was interesting to compare statistics for the different continents, both in terms of total numbers of certificates and in more absolute terms as certificates awarded per capita. Again, the most recent figures (June 2009) are chosen here, but other months show a similar pattern. These are absolute figures, not per capita

Continent/area	No. of certificates
Africa	11
Asia (Middle East)	77
Asia	4411
Australasia	30
Europe	1002
North America	127
South America	35

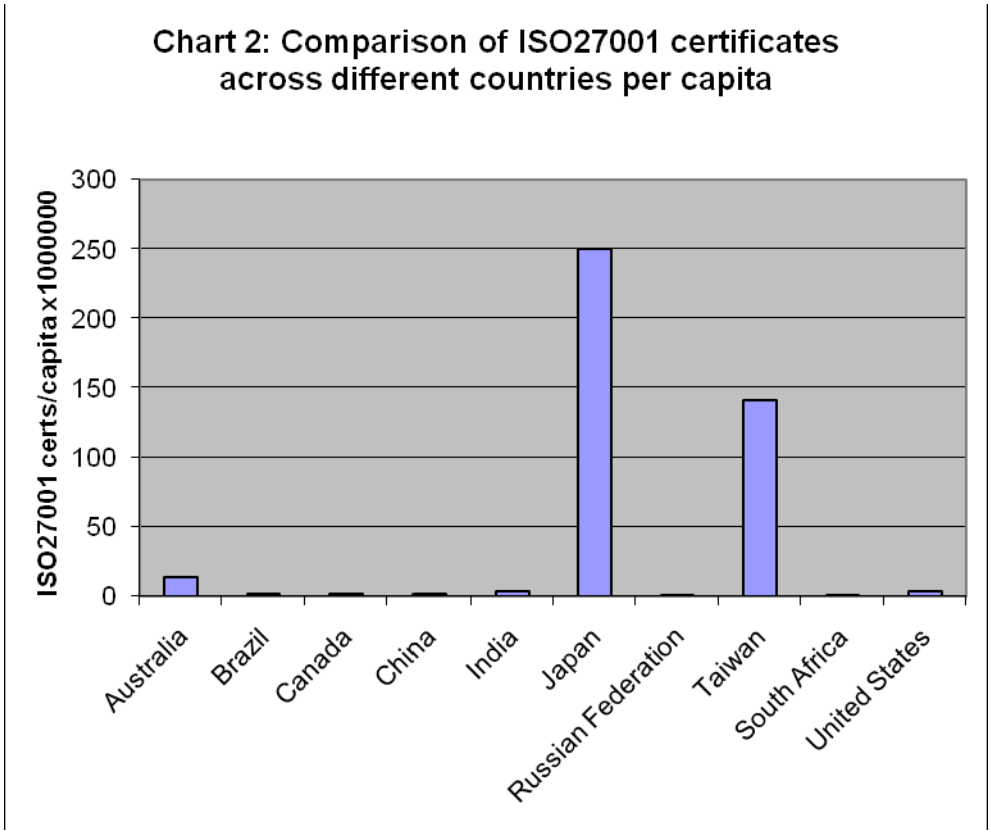
Table 4: ISO27001 data for different continents taken at the end of June 2009

As with European figures, the variations were considerable, but this is much more as expected because of the greater difference in GDP of these continents. What is noteworthy is the very high figure for Asia.

Asia is a very large continent. To investigate further, particular “exemplar” developed countries within and outside Asia were chosen to compare the effects per capita already perceived with the European statistics (Table 5, illustrated in Chart 2).

Country	No. of ISO27001 certificates	No. of ISO27001 certificates per capita
Australia	29	0.0000133
Brazil	22	0.0000012
Canada	5	0.0000015
China	199	0.0000015
India	454	0.0000039
Japan	3191	0.0002500
Russian Federation	10	0.0000007
Taiwan	325	0.0001411
South Africa	5	0.0000010
United States	94	0.0000031

Table 5: ISO27001 data per capita for chosen non-European countries taken at the end of June 2009



The figures taken from Table 5, and illustrated in Chart 2 show some quite astonishing differences, revealing where much of the Asian growth is and is not taking place. They show that Asia/Far East countries like Japan and Taiwan are quite clearly leading **the rest of the world** in the development of organisational ISMSs. The reasons why Japan and parts of the Pacific rim should be so advanced in terms of certificating their ISMSs is worthy of investigation because the results of such a study may lead to greater understanding of the wider organisational problems affecting global information security.

Statistics for ISO27001 take up in different countries as the recession started to take effect

Although economic activity has been falling in recent months, it is interesting to look at trends in ISO27001 growth, as a measure of the extent to which the recession has been hitting progress with the development of more robust information security management systems.

As previously stated, with the exception of the US, GDP comparison figures for different countries started to become negative during the latter half of 2008. Figures obtained for ISO27001 certificates issued over all countries in recent months can therefore be related directly to the fluctuating GDP in that country to see whether the recession is indeed having an effect.

Thankfully, records of ISO27001 certificates issued have been issued on a monthly basis since late 2008 (for latest see ISMS, 2009), so it was possible to make a comparative study of individual countries and continents over a period of several months.

Continent/area	Dec 08	Feb 09	Apr 09	June 09
Africa	8	9	11	11
Asia (Middle East)	66	67	70	77
Asia	3868	4053	4110	4411
Australasia	29	29	30	30
Europe	874	909	973	1002
North America	104	107	108	127
South America	34	32	34	35

Table 6: Total ISO27001 certificates awarded on different continents/areas since the recession started to have a global effect

Analysis of the results of this unique study show the following trends in ISMS development behaviour as the recession has taken effect around the world:

1. Growth is continuing at a slow, but steady rate in Europe, in spite of the recession
2. Growth is continuing at a fairly fast rate in Asia, particularly around the Pacific rim, and again in spite of the recession
3. Other continents have much slower growth

This presents a complex picture and it is difficult to draw specific conclusions. Although countries are already emerging from recession, the full effects on ISO certification rates may not yet have filtered through to because it can take one year or more for an organisation to go through the whole process of developing/implementing an ISMS. Organisations becoming certified now may have started their project 6 – 24 months ago. In countries where motivation is purely cash flow and profitability it may be expected that the state of the economy will have a significant effect. However those countries where culturally the motivations for information security may be more aligned to CSR, ethics, personal shame, etc may not see such a strong link with current recession concerns.

Why such big differences in ISO27001 take up in different countries with similar GDP regardless of the recession?

The announcement of the ISO27001 ISMS standard (ISO, 2005) received considerable acclaim, and was recommended in a significant UN report (UN, 2005). A number of researchers helpfully provided evidence why ISO27001 and the formal adoption of an ISMS approach would be helpful to organisations, and why it may provide a cost-effective long-term solution (e.g. Coles-Kemp & Overill, 2007). More recently, researchers (Bartlette & Fomin, 2008) have commented on the disappointing growth levels of ISO27001 certificates awarded in EU countries compared to other International standards such as ISO9001, and broadened their study the following year (Fomin, de Vries, & Barlette, 2008). The current paper uses more detailed data; perceived differences between apparently similarly developed countries will be analysed from an economic perspective, and in terms of the needs of SMEs. Many developed countries have 75-80% of their GDP created by SMEs, and the drop in output during a recession will include a drop in SME output. Whilst the rest of this study may be inconclusive about effects of the recession, it has revealed some fascinating anomalies between countries, which may be of use to practitioners in those countries where ISMS growth is currently very low.

Economic Drivers for ISMS development/certification

The rest of the paper will focus on economic drivers for organisations and look at how these drivers may or may not have importance in particular parts of the world.

(1) Legal and Regulatory Drivers

The recent Ernst & Young (2008) survey noted that regulatory compliance has been the leading driver for information security since 2005. Although this is about the time that organizations would be considering starting to work towards the then new ISO27001 certificates, no regulatory or statutory legislation **specifically** mandates ISO27001. Most require "reasonable & appropriate" measures to be taken. ISO27001 is seen as a benchmark of taking reasonable and appropriate measures.

Three legal and regulatory drivers can readily be identified:

(a) data protection legislation
(b) privacy disclosure legislation
(c) on-line credit card use security framework, known as PCI DSS.

Of these, the first two are country-specific, but the last is global.

(a) Data Protection Legislation in the UK, and elsewhere in Europe

A summary of the UK Data Protection Act is provided as appendix 1. These changes were brought about in anticipation of a seven-year holiday of prosecution ending in 2005. The UK data processing law is generally accepted, even by the ICO (Information Commissioners Office) itself, as being among the weakest in the EU. The reasons for that are social and political as well as economic and beyond the scope of this paper. A comparative study covering SME practice in dealing with personal data covering several European nations from the 1981 EU directive to present day would be very useful in this regard. However, the repercussions of not doing so according to stronger data protection legislation elsewhere in Europe has not sufficiently motivated those responsible for securing data to do so to stop or reduce the incidence of data breaches occurrence.

A similar pattern of personal data protection occurs in many developed countries. Some examples are given below:

Japan has progressively exercised more central control:
1998: The Privacy Issues Study Working Group produced 'Guidelines concerning Protection of Personal Data in Electronic Commerce'.
2000: Another Study Group on Personal Data Protection produced an Interim Report
2003: Personal Data Protection Legislation Special Committee formulated a legal framework and the Personal Information Protection Law
2005: Personal Information Protection Law **obligations** of businesses took effect (Pishvar et al, 2007)

Turkey introduced data protection legislation in 2003, probably to bring that country closer to Europe. Effects on controls on information security are discussed by Cebi et al, (2007).

Canada acted to protect data earlier than the EU, in 1980, and adjusted laws to bring them in line with Europe to allow free trade in 2002.

Data Protection Laws can of course only be effective if there is a sizeable chance of being caught, and the fines imposed are significant.

United States has no specific Data Protection legislation was passed by the senate, but the HIPPA act (1996) was brought in to safeguard and protect healthcare data. In 2002, they introduced the Sarbanes-Oxley (SOX) legislation (US Federal Government, 2002), protecting financial data.

(b) Privacy Disclosure Legislation

The State of California introduced data disclosure legislation soon after SOX, and other US states followed suit over the following years, which may again explain why the Ernst & Young study regarded 2005 as being a significant legislative year. Because there was no data protection act in the US, personal data (other than financial and healthcare data) had no protection at all before SOX came into being.

Some businesses did not and do not like the SOX legislation, and wish even now to see it removed on the grounds that it costs the businesses money that they cannot afford to pay during the recession. This reinforced the worry implied in the title of this paper that businesses would prefer not to spend money on information security, and the recession might give them that excuse not to do so – or to delay setting up an ISMS until the economy has picked up.

Perhaps surprisingly, organisational objections to SOX have recently been used by the UK ICO to support a lobby to prevent the introduction of similar disclosure legislation throughout the EU by 2012, although debate on this matter continues. In any case, this legislation is not about to happen and is unlikely to have an immediate impact on businesses.

(c) Credit Card Regulations, PCI DSS

The Payment Card Industry Security Standards Council (essentially Visa and Master Card) first introduced a set of guidelines known as PCI DSS (Payment Card Industry Data Security Standard) for the beginning of… 2005. Now, after several years, they have taken many organisations "off guard" by choosing to enforce the regulatory aspect worldwide from 1st October 2009. This change was announced in September 2008 giving an organisation working from scratch one year to develop an ISMS to meet the guidelines. It is interesting, but perhaps coincidental, that PCI DSS was tightened at the same time that the recession started to effect business outputs. It could be that in the short-term the recessionary and PCI DSS effects will cancel each other out in terms of the rate of uptake of ISO27001 certification. The longer term effects of PCI DSS can only be speculated, but it seems likely that this will be a powerful ISMS driver globally for any organisation that deals with payment by credit card and has not made the required efforts to comply with standards or legislation (PCI Security Standards Council LLC, 2008). PCI DSS is nothing like as stringent as ISO 27001 and uses a different methodology, but some organisations may take the opportunity to develop an ISMS that meets the requirements of the ISO27001 standard.

(2) Protecting Reputation and Brand

The Ernst & Young survey (2008) reported that protection of reputation and brand has increased considerably since their 2007 survey. It therefore appears that this has become a significant driver for information security. This could partly be a consequence of the Californian "disclosure" law relating to the Sarbanes-Oxley Act, and partly because of a concern about bad publicity as a result of the media exposure that would follow a data breach (HMSO, 2007).

However, it could also be a result of the good publicity gained from becoming certified. For example, from the evidence of at least one Japanese company report (Sony Financial Holdings, 2008), getting ISO27001 accreditation during 2007 is considered with pride as positive news to report to shareholders. It appears that this is currently a cultural matter, but could be a future driver for Western companies to contemplate.

(3) Market Pressure

If market rivals are gaining customers as a result of getting and advertising ISO27001 certification, pressure comes to bear to do likewise. The example quoted above provides evidence that ISO27001 is being proclaimed in Japan (Sony Financial Holdings, 2008), although this seems currently more to be an issue of boosting the brand rather than in response to the action of market rivals. If Sony Financial Holdings' market rivals have moved towards ISO27001 certification recently, then market pressure could be a factor. The combined effects of improving the brand with ISO27001 and market pressure to compete will together act as powerful drivers towards certification.

Also, if business supply chain partners require ISO27001 certification, that will provide a reason to move towards being certified. More research required to see whether this is affecting certification behaviour in Japan.

(4) Physical Cost of a Breach

This is the powerful ROI (Return on Investment) argument, with the suggestion that, over a period of time, compliance will have the effect of saving money. Even before "Economics of Information Security" research became available, it was possible to provide qualitative data that would support the concept that specific spending on protecting large company data made good common sense. The question now was… how much should they spend to safeguard their data? The data breach protection as a ROI argument can only work if a data breach is taken as a medium-term statistical certainty if protection is inadequate.

Prior to 2002, the physical cost of losing digital data was often never really assessed, and possibly regarded as negligible. An ROI argument was therefore difficult to justify without evidence. However, in recent years, when huge amounts of data can be stored on a portable medium, more enlightened organisations have acknowledged that there may be a sizeable cost involved in gathering and maintaining their data, and in data recovery if corporate data is lost. Such organisations rightly regarded such data as an asset, the protection of which should automatically be factored into any risk assessment process. Once an organisation had got to the stage of involving information in a risk assessment, it was already on a recognised path towards developing an ISMS. A number of researchers were able to move the knowledge base forward in this area; particularly influential was the work of Gordon & Loeb (2002), which, in their own words:

"… presents an economic model that determines the optimal amount to invest to protect a given set of information."

(Gordon & Loeb, 2002, abstract)

As the discipline moved forward, not only was it possible to establish that a data breach involving corporate data will have a financial impact, but Professor Ioannidis (2005) derived a formula to quantify this. Also, Acquisti et al (2006) built on Campbell et al's earlier work and did some ground-breaking research in providing a formula for estimating the cost of a corporate data breach on an organisation's stock market price. Rowe & Gallaher (2006) wrote about return of investment by an organisation also including contributing to knowledge (the public good) through focusing on costs in this way. This is fine for larger corporate organisations that can give something back to a wider community, and support organisations wishing to promote and mitigate against the social effects of Cyber crime. However, it is doubtful whether, without external encouragement, such altruism would be high priority for an SME.

It has not been particularly well publicised that formulae are indeed available to SMEs to estimate the cost of data breach. In our view, it is also helpful to analyse SME data as personal and corporate data, looking at the various consequences of losing each type, and gauging singularly and in total the impact of losses on profitability. For example, a single record can now be given a value based on current estimates of its black market value. Applying a conservative value of - say £50 - to a personal data record even a small company can rapidly become aware that the contents of its customers database has a considerable value. The typical SME could equally suffer loss or corruption of customer data, of organisational data, or both. SMEs are indeed collectively in a position to be able to provide useful data to researchers, assuming that the data obtained would be suitably anonymised before being used. However, within the harsh reality of the SME, and their owners, motivations may be economic to the extent that they are more interested in their own future profitability than in helping other organisations:

"SME's are usually run by entrepreneurs who view information systems and technology as tools that can be used to assist in running a business more efficiently."

Upfold & Sewry (2005)

They would expect government-backed bodies to assist and encourage any such engagement, and provide relevant information.

(5) Effect on Stock Market Value

A year after Gordon & Loeb produced their landmark 2002 study; the same authors working with Campbell published clear evidence that data breaches could also affect a company's stock market price (Campbell et al, 2003). Although the drop may only be short-lived, it could affect public confidence and reduce sales. Since 2007, public sensitivity to loss of their data has increased, and effects could be more dramatic.

(6) Effect on Insurance Premiums

The idea of insuring against data loss is examined by Kesan et al, 2005, and would appeal to any organisation. However, now that calculations involving risk of data loss are available, the process is considered by some to be analytical enough to consider an actuarial approach to providing information risk insurance premiums (Herath & Herath, 2007).

(7) Outsourcing

This has particular financial attractions for SMEs, and further attractions for those not wishing to engage too much with the ever-changing technology. This could be perceived as a way of cutting costs by a business seeking to keep expenditure to a minimum. However, the research findings of Khalfan (2004) suggested that such an approach may have a negative effect on information security, and the "false economy" of increased chance of data breach should again be factored in.

The same sort of arguments should be applied to the current vogue of "outsourcing to the cloud", a topic getting a lot of attention and of interest to SMEs because it renews the "expenditure reduction" allure of outsourcing in general. In practice, all types of outsourcing require third party risk management, and cloud computing is no exception. However, this can only be done accurately if the value of the information asset is reasonably assessed.

ISMS "maturity" modelling for SMEs: moving beyond the costs of Losing Data towards an acceptance that "it is good for the business"

It has been clearly identified in the research that the smaller the business, the less likelihood there is that they will undertake information risk analysis (Dimopoulos et al, 2004). Research suggests that an increasing number of businesses have an

Information Security Policy but does not investigate the issues involved in requiring an SME to undertake information risk analysis, and there is the problem with progression beyond that first stage. The current situation for SMEs in the UK (a better than average country in terms of ISO27001 certification) was summed up in the following way by Bruce Hallas, one of the authors of this paper during a seminar for the ESRC (Economics and Social Research Council) at HP Labs last year:

"… SMEs are particularly prone to poor or even non-existent information security. As awareness of the importance of information security increases, the SMEs stand to lose competitiveness, potentially losing contracts with existing clients and suffering the financial consequences that are increasingly arising from information security incidents." (ESRC, 2008, p.1)

SMEs have typically been less likely to be dependent on complex information systems, and some may even still employ the old practices of filing corporate data away safely in a lockable cabinet. However, an increasing number of SMEs do now use online shopping, keep electronic customer records, and allow payment by credit card. In these recessionary times, when they are strongly in competition for market share of a dwindling cake, a PCI DSS breach could put an SME out of business. They may not afford ISO27001, but at least an information risk assessment is needed.

Conclusion

The research findings here are inconclusive regarding recessionary effects on ISMS development. However, this research has also revealed the extent to which many advanced economies have been falling well behind those in the Pacific Rim and particular parts of Europe in terms of protecting organisational data. Pre-2005 legislation encouraged organisational compliance but recently North America and most of Europe seem to have preferred a free market approach to ISMS development.

By contrast, an impression is created that Taiwan and Japan are more "hands on", seeking to utilise academic models to help educate organisations so they can engage with ISMS complexity. In Japan, Tanaka et al (2005) provided some thought-provoking analysis regarding the financial implications of good security in the use of e-government. One wonders about the impact of this paper in terms of the subsequent encouraging ISO27001 accreditation in that country. In Taiwan, an educational maturity model (ISEMM) has been developed to assist organisations develop ISMS expertise (Chiang et al, 2008), and the expertise developed is being shared (Ku et al, 2009). The Austro-Hungarian effect is also worthy of investigation, to see if the same drivers are working as in the Pacific Rim. Academics perhaps underestimate the influence that they can have on policy making. The effects of good national leadership in encouraging improved ISMSs and organisational ISO27001 certification and would appear to be self-evident, but economic drivers are also identified as important.

References

Acquisti A, Friedman A, and Telang R, 2006, “Is There A Cost To Privacy Breaches? An Event Study”, WEIS 2006. Available at: http://weis2006.econinfosec.org/docs/40.pdf

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

Bergman A, Verlet A, 2006, “Security breaches: to notify or not to notify – that is the question”, Network Security, Volume 2006, Issue 5, May 2006, Pages 4-6.

BERR, 2008, “2008 Information Breaches Survey: Technical Report”, Executive Summary, pp8-9. Available at: http://www.berr.gov.uk/files/file45714.pdf

Boehmer, 2008**, “**Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001”, Emerging Security Information, Systems and Technologies, 2008. SECURWARE '08. 2nd International Conference.

Campbell K,. Gordon L, Loeb M, and Zhou L, 2003, “The economic cost of publicly announced information security breaches: empirical evidence from the stock market” in Journal of Computer Security vol 11.3.

Cebi Y, Tahaoglu OO, 2007, “Personal Data Protection in Turkey: Technical and Managerial Controls in Security of Information and Networks”, Proceedings of the First International Conference on Security of Information and Networks (SIN 2007), pp.220

Chiang T J, Chang Ray-I, Kouh J S, Hsu K P, 2008, “An Information Security Education Maturity Model”, 2008 International Conference on Computer & Network Technologies in Education (CNTE2008), pub: 25-31 Aug. 2008, pp.224-231.

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”.

Dodt A, 2008, “ROI more important than ever”, Infosecurity Volume 5, Issue 7, October 2008, Page 4

Ernst & Young, 2008, “Moving Beyond Compliance: Ernst & Young 2008 Global Information Security Survey, p.6. Available at http://www.ey.com/Global/assets.nsf/UK/Global_Information_Security_Survey_2008/$file/EY_Global_Information_Security_Survey_2008.pdf

ESRC, 2008, “Press Releases, 2008, June: Wake-up call to business: Tighten up on Information Security”, ESRC Society Today, June 2008.

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

Federal Office for Information Security, 2004, “IT Grundschutz Manual”. Available at http://www.bsi.de/english/gshb/manual/download/modules.pdf

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

Gordon L. A., & Loeb M. P., 2002, “The Economics of Information Security Investment”, ACM Transactions on Information and System Security, Vol. 5, No. 4, November 2002, Pages 438–457.

Herath H S B & Herath T C, 2007, “Cyber-Insurance: Copula Pricing Framework and Implications for Risk Management”, WEIS 2007 Conference. Available at http://weis2007.econinfosec.org/papers/24.pdf

HMSO, 1998, “Data Protection Act”.

ISACA, 2007, “COBIT 4.1 Executive Summary”. Available at http://www.isaca.org/AMTemplate.cfm?Section=Downloads&Template=/ContentManagement/ContentDisplay.cfm&ContentID=34172
ISMS, 2009, “International Register of ISMS Certificates, Register Search (Version 18 February 2009)”. Available at http://www.iso27001certificates.com/
Kluge D, Sambasivam S, 2008, “Formal Information Security Standards in German Medium Enterprises”, The Proceedings of CONISAR 2008, 1533, pp.1-12. Available at http://isedj.org/isecon/2008/1533/index.html
Ku C-Y, Chang Y-W & Yen D C, 2009, “National information security policy and its implementation: A case study in Taiwan”, Telecommunications Policy, Volume 33, Issue 7, August 2009, Pages 371-384
Nagata K, Amagasa M, Kigawa Y, Cui, 2008, “Risk Evaluation for Critical Assets with Fuzzy Inference Mechanism in an Information Security Evaluation System”, Proceedings of the 9th Asia Pacific Industrial Engineering & Management Systems Conference pp 2630-40. Available at http://www.knu.edu.tw/lecture/2008%20APIEMS(BALI)/PAPER/319-79.pdf
Pishva D, Kitamura N, Tsugawa S, Takeda K., 2007, “An Initiative to Improve the State of Information Security at Local Governments in Japan”**,** Proceedings of 2007 41st Annual IEEE International Carnahan Conference on Security Technology, Volume, 8-11 Oct. 2007 pp. 8-17. Available at http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?isnumber=4373447&arnumber=4373461&count=51&index=4
Price-Waterhouse-Coopers, 2008, “Safeguarding the new currency of Business”, p.2. Available at http://www.pwc.com/extweb/insights.nsf/docid/0E50FD887E3DC70F852574DB005DE509/$File/Safeguarding_the_new_currency.pdf
Schneier, B, 2002, “No we don’t spend enough”, WEIS2002. Available at http://www2.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/18.doc
Sony Financial Holdings, 2008 Annual Report. Available at http://www.sonyfh.co.jp/en/financial_info_e/ar_e/080812_01.pdf
Tanenbaum, D, 1988, “Computer Networks – 2nd edition”, Prentice-Hall

Appendix 1: Summary of the UK Data Protection Act 1998

Summary of the Data Protection Act 1998

The Data Protection Act sets out eight protection principles which form the legislative framework and with which a data controller must comply.
1st: Personal data shall be processed fairly and lawfully.
2nd: Personal data shall be obtained only for one or more specified and lawful purposes.
3rd: Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4th: Personal data shall be accurate and where necessary, kept up to date.
5th: Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.
6th: Personal data shall be processed in accordance with the rights of data subjects under the Act.
7th: Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data.
8th: Personal data shall not be transferred to a country or territory outside the European Economic Area…

Interpretation of the 7th principle

The Seventh Principle of the Act states that "appropriate technical and organizational measures" must be taken to protect personal data, and gives advice on appropriate security measures.