

**Athens Institute for Education and Research**

**ATINER**



**ATINER's Conference Paper Series**

**SME2013-0547**

**A Model for Proactively Insuring  
SMEs in the Supply Chain against  
Cyber Risk**

**Richard Henson**

**Worcester Business School**

**Duncan Sutcliffe**

**Sutcliffe & Co. Insurance Consultants**

**UK**

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

Printed in Athens, Greece by the Athens Institute for Education and Research.  
All rights reserved. Reproduction is allowed for non-commercial purposes if the  
source is fully acknowledged.

**ISSN 2241-2891**

19/09/2013

## An Introduction to ATINER's Conference Paper Series

ATINER started to publish this conference papers series in 2012. It includes only the papers submitted for publication after they were presented at one of the conferences organized by our Institute every year. The papers published in the series have not been refereed and are published as they were submitted by the author. The series serves two purposes. First, we want to disseminate the information as fast as possible. Second, by doing so, the authors can receive comments useful to revise their papers before they are considered for publication in one of ATINER's books, following our standard procedures of a blind review.

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

This paper should be cited as follows:

**Henson, R.** (2013) "A Model for Proactively Insuring SMEs in the Supply Chain against Cyber Risk" Athens: ATINER'S Conference Paper Series, No: SME2013-0547.

## **A Model for Proactively Insuring SMEs in the Supply Chain against Cyber Risk**

**Richard Henson**  
**Worcester Business School**  
**Duncan Sutcliffe**  
**Sutcliffe & Co. Insurance Consultants**  
**UK**

### **Abstract**

There has been increasing concern in recent years about the lack of urgency in SMEs regarding security of their information. Concern stems not only from the risks the SMEs are taking not only with their own data, but also with the data they share with supply chain partners. Current surveys have shown that the situation is getting worse with human error compounded by cybercriminals exploiting weaknesses in SME systems and using them to hack supply chain hubs.

In this paper, a researcher and a practitioner from the UK investigate possible reasons for SME apparent lack of interest in securing data, or developing information security management systems (ISMSs). In the absence of UK legislation, the only way SMEs are likely en masse to improve their information security is through pressure from supply chain partners and particularly supply chain hubs. The authors present an interesting development in cyber liability insurance which provides the basis for a cost-effective solution that will encourage good information assurance across the supply chain.

The solution offered in association with a major International insurer is explained in detail in this paper. It has the dual advantages for participating SMEs of ensuring that they develop a level of information assurance that will offer them actual protection, and at the same time provide them with insurance that will protect them financially against data breaches or other costly consequences of weak information security. The scheme used will provide actuarial evidence for the insurer to further refine the model. Clients that cannot show evidence of a base level of security will not get insurance cover; by contrast those assessed as being more secure will be eligible for a discount. The tool used is a self-assessed version of the IASME information assurance standard, and participating organisations will also get an IASME discount. IASME was recently developed in the UK to meet the needs of SMEs wishing to safeguard their precious information but not possessing the resources to achieve the ISO27001 standard.

**Keywords:** SME, Information Risk Management, Information Assurance, ISMS, Information Security Management Systems, Data Protection

Legislation, Economics of Information Security, Supply Chain, Standard, ISO27001, IASME, Self-assessment, Insurance, Cyber Liability

**Corresponding Author:**

## **Background**

Information security researchers and consultants around the world looked on with incredulity as the highly secure mainframe computer environments of the 1980s were gradually replaced by Local area networks (LANs) with localized data processing and storage. The biggest danger was that anyone could merely copy confidential data and save it under another name, and such a massive change would need government intervention to ensure that these new powers with regard to confidentiality were not abused.

Different countries had different responses. In the UK, there was a perception that the newly introduced Data Protection Act (HMG, 1984) would ensure that personal and confidential data was not misused. This was itself a response to EU Directive from 1981. However, the directive was created at a time when computing was almost exclusively centralised and based on mainframe computers based in a separate data processing department. At that time, smaller companies did not use computers at all.

By the 1990s, the situation had been further complicated by the use of larger mass storage devices such as CDs, and the connection of individual and LAN-based computers to the Internet contributed to creating a global information system that was completely out of control. Researchers, governments, and security product manufacturers provided plenty of evidence of the extent of information mismanagement, and the ease with which hackers could obtain information, but they were generally ignored. Smaller organisations gradually used personal computers, and some even started to link them together for processes of information sharing.

## **The Emerging Problem in Detail**

As time went on, expertise was shared and solutions were generally adopted. Whilst misuse of data within an organisation was a management problem, larger companies and government departments assessed that their respective IT departments were closest to the data, and therefore best able to deal with the emerging information management problem associated with electronic data. This was to some extent ironical because it was usually the IT departments that had told their respective managements that the removal of read only centralised computing, end-user empowerment, and local storage would, without proper user training, present a security problem, and had been largely ignored. Now the problem was finally acknowledged it was left to those same departments to solve it. Of course SMEs often didn't have an IT department, so the problem was often not addressed at all, other than a reminder about the Data Protection Act.

Around the world, governments offered different responses to the quietly acknowledged but growing problem with personal computer network and Internet based organisational computing:

1. Legislate (but how to enforce?)
2. Educate (but who is going to pay?)
3. Offer and encourage codes of practice & regulations (again, how to enforce?)

One response was to develop a code of practice further into a process-based approach to information security, which could be certified. The carrot would be that the certificate would show good information management, and improve an organization's reputation, and subsequently their customer base. The most effective of the many standards that emerged was developed in the UK from best practice of government departments. This set of security controls and guidelines for information security processes became a British standard, known as BS7799.

#### *Adoption of Information Security Standards*

Although excellent for larger companies and public sector departments, it was acknowledged that BS7799 wasn't designed for small and medium-sized enterprises (SMEs). It was a very cumbersome standard, which would be expensive to develop and maintain, and beyond the financial and human resource reach of smaller organisations. Surprisingly, very little government advice was offered to these SMEs, which were rapidly growing in numbers, and providing an increasing percentage of a typical country's GDP.

Within and beyond organizations, crimes were increasingly being committed through exploitation of data. In most countries governments were reluctant to intervene, with the general mantra being let the emerging information superhighway police itself. Most of on-line transactions were completed with the aid of credit card numbers, and this became lucrative for credit card companies who had no wish to discourage such activities and offered compensation to consumers and businesses alike in the relatively small numbers of cases of fraud. However, As the millennium approached, and passed, information security problems continued to rise. The new academic discipline of "Economics of Information Security" emerged in response to the fact that even larger organisations weren't aware of the extent of the problem, the economic case for doing something about it, and the relative benefits of different actions to help secure organisational data.

Some countries considered a more serious view about data misuse, and introduced stricter legislation e.g. Japan, United States of America (starting with California)

Governments in most countries were reluctant to legislate in this way, probably because of fear or an organisational backlash at a time when a new market was emerging, and the cost of adequately policing any such legislation. The typical approach was to offer advice to businesses and organisations, and to recommend compliance with a security standard. Although BS7799 was popular, compliance with other standards and codes of practice such as COBIT, ITIL and ISF were (and still are) also popular, and encouraged.



Unsurprisingly, crime involving the misuse of data continued to increase throughout the 2000s decade throughout the world. The authors are based in the UK and remember newspaper headlines based on data breaches appearing on a fairly regular basis from mid-decade. Statistics available from that era showed a big rise in e-crime (as it became known), supporting the perception from the Information Security community that the information ecosystem was being exploited more and more frequently. There was a slight tightening of penalties under the Data Protection Act (DPA), and some resources made available to the public sector for awareness training, but that was about it.

One great hope for researchers and practitioners involved in securing the information ecosystem was the emergence in 2005 of an International Standard (ISO27001) to certify organisations who have developed a robust information security management system (ISMS). However, the International Standard was based around BS7799 and suffered from the same limitations. ISO27001 certification levels in the UK and in most countries round the world have to date been remarkably low. One of the authors (Henson and Hallas, 2009) noted at a previous SMEs conference that the only ISO27001 hotspots emerging were in the Pacific Rim and Eastern Europe. Indeed, the latest statistics (ISMS, 2012) show that to still be the pattern today. The message for the would-be hacker is clear: target servers in a country with low take up of security standards, and poor data protection legislation, poorly policed.

The cost to the UK of all this cyber criminal activity has been estimated (Detica, 2011) at £27billion. Other more recent research (Moore, 2012) suggests a figure that is somewhat lower, but the research also reveals surprisingly low apprehension rates.

“The straightforward conclusion to draw on the basis of the comparative figures collected in this study is that we should perhaps spend less in anticipation of computer crime (on antivirus, firewalls etc.) but **we should certainly spend an awful lot more on catching and punishing the perpetrators.**

If this interpretation is correct, then cyber crime is now the typical volume property crime in the UK, and the case for more vigorous policing is stronger than ever.”

This is of course the inevitable result of twenty years of essentially letting the market decide, with weak legislation poorly enforced. The findings and conclusions of Moore, Anderson et al were not considered as helpful; from an information security perspective it is difficult to see why.

### **What can be done?**

One obvious response would be to accept the emerging consensus and tighten up legislation, and the policing of existing legislation. After a series of passionate debates, this appears to be the approach adopted by the EU Parliament and regulations are due to come into force. Sadly, the UK data protection enforcer does not feel that it can be policed () unless massive extra

resources are employed. Various studies have shown the extent of e-crime in the UK (up to £27 billion), and the very small amounts being spent on catching the criminals. Other studies have shown a change in the behaviour of credit card companies; whilst the consumer is protected, vendors have to meet the cost of unproven fraud for themselves, and comply with the credit card companies own regulations, PCI-DSS (PCI Security Standards Council, 2008). The penalty for non-compliance is having their on-line credit card license revoked. In even quite recent research, surprisingly few SMEs were even aware of PCI-DSS or aware that the regulations could impact on them.

In the absence of a government lead, other than acknowledging that this is a big problem and providing small amounts of financial support for awareness training, three approaches to solution have been and are being adopted:

1. Let the market decide what to do
2. Use supply chain hubs to get SME security in order
3. Use cyber liability insurance, coupled with discounts for achievement against a security standard

#### *Addressing B2B Market Failure*

As already implied, SMEs are very reluctant to engage at all with spending on information security in any consistent way other than purchase of hardware and antivirus and related software. Why are UK businesses and organizations so reluctant to go a little further with their spending, take appropriate precautions to systematically store data and then get a badge for doing so? Smaller businesses must hear of all of the threats presented to them by security industry, and to the external observer it must be quite baffling why they steadfastly refuse to spend appropriately and wisely on protecting their precious data against all these threats. It can't be that they are "anti-badging" because very many of them have acquired ISO9001 certification, awarded for their great efforts towards achieving good quality management systems. Perhaps the information security management badge is seen as too difficult to get, but more likely, according to industry research (), they still don't want to engage with, let alone understand the problem.

As reported in previous research (Henson et al, 2011) one of the authors conducted research on local (Worcestershire) businesses in an effort to find out whether a lack of appropriately priced courses that they could send their staff on was the problem? The responses suggested that most just weren't interested in spending time and money on steps to secure their data. They saw it as an unnecessary additional cost that would not give them any market advantage. However, others did show some concern about data breaches, but were put off by high costs of getting certified to a recognizable standard like ISO27001. This backdrop, and possible economic drivers for changing SME behaviour, were described for a paper at a previous Atiner SMEs conference (Henson & Hallas, 2009). At this point in time it was expected that the continual stream of information about data breaches would bring about a change in attitudes and higher adoption of ISO27001 in the UK. However, the research also showed

that a less cumbersome system than ISO27001 would be beneficial to SMEs. More recently, Henson et al, 2011, explained a newly developed standard especially for SMEs, which became known as IASME (Information Assurance for SMEs).

IASME is generally recognised as being an appropriate product, enabling the business to develop an information security management system relatively slowly, and at modest cost. It has also been well advertised and promoted round the country on "road shows". However, the take up to date has been disappointing. The IASME team accept that it is still early days, and a new product will always take time to get brand awareness. Nevertheless, many businesses clearly don't seem to be prepared to spend even the modest figure of £2500 (price for a micro business) to shore up their defences.

Nor is it specifically IASME or ISO27001 that SMEs are rejecting. The UK government has, in 2013, made £5000 innovation vouchers available to SMEs for a variety of options to improve aspects of information security, and whilst interest has been steady, there has been no rush to take up these vouchers. If the market is left to its own devices, in some cases people steer away from things that are good for them. It appears that information security is one of these areas. A researcher from a 2005 WEIS (Workshop on Economics of Information Security (WEIS) conference concluded that "network security appears to have properties of a public good" (Bohme, 2005), and inferring that regulation is necessary as a challenge to the market failure.

In the authors' opinions, the best summary of the SME lack of interest in information security is therefore indeed "market failure", and steps need to be taken urgently to change this dangerously complacent attitude.

#### *Real and Present Danger*

The danger of market failure is that something important can be prevented from growing through cultural norms that have emerged and are resistant to change. It is now increasingly accepted among researchers and relevant professionals that there is a potential vulnerability to UK infrastructure through the supply chain. Whilst the larger companies at the heart of the supply chain can (and do) spend massively on information security because they understand the risks, the SMEs in that supply chain don't have either the resources or the perceptions of danger that the organisation at the hub of the supply chain will (or should!) have. With Internet-based trading more and more common, supply chains are often becoming global, with SMEs from a number of countries involved. It only takes one of these SMEs to present vulnerability or the hackers to get potential access to the hub. The best documented example of this happening was in the US, where plans for a military aircraft design were hacked from a supply chain hub, and it turned out that a recruitment agency associated with the supply chain provided the hackers with a route in, which was duly exploited. The government concerned (the US) responded swiftly, but pointed the finger at supply chain hubs as needing to be more responsible concerning with whom they do business, and to make sure their partners are secure against attack. However, there was no new legislation. After all, the US

was already one of the best-legislated countries against data breaches, with its own data breaches law operating in most states ( ).

The effects of supply chain pressure are slowly being felt, as businesses realise that to do business with particular supply chains they have to show compliance with information security management principles. Historically these have been through self-checking exercises, but indications are emerging that (particularly in the US) the expectations placed upon SMEs from an information management and security perspective are becoming more demanding. As supply chains are increasingly global, countries with a business culture that respects information security can be expected to gain more contracts than those who "let the market decide".

#### *Emergence of Cyber-Liability Insurance*

The most influential thinker in Economics of Information Security is probably Ross Anderson, of Cambridge University, who has written dozens of papers on the subject, and jointly founded WEIS in 2001 with prolific thinker and writer Bruce Schneier. However, long before he produced "Why information security is hard – an economic perspective" (Anderson, 2001), the seminal paper that inspired WEIS, Ross said:

"A trusted component or system is one which you can insure."  
Anderson, 1994)

Cyber Insurance featured regularly at the annual WEIS conferences. In a paper presented at an earlier ATINER conference (Henson & Hallas, 2009), insurance premiums were identified as one of six possible business drivers for security spending (the other five are compliance with laws & regulations, protection of brand and reputation, the physical cost of a breach, market pressure for a standard, and stock market price). At that time there was only very limited choice of insurance in the UK, and aimed at a very limited market. The cybersecurity market was not understood at all by buyers or sellers.

Throughout many years, the offer of insurance has been successful in making a breakthrough in cases of perceived market failure, and it made perfect sense for insurance companies to devise products that would be attractive to organisations concerned about the costs of a data breach. As already mentioned, the UK seems to be well behind the leading-edge countries in terms of all things cyber security, and insurance products are only just starting to emerge; in other parts of the world, over 10 years ago, innovative products were being developed for secure institutions based on an acceptance of the impossibility of total security, and providing some recompense in the unlikely case of such a breach (Siegel et al, 2002). A framework for more widespread cyber security liability insurance soon followed (Gordon, Loeb, et al, 2003). Soon afterwards, in a groundbreaking paper, an academic asked the question

“... is there a business model for insurance companies to offer coverage against damage caused by worms and hackers at acceptable premiums?” (Bohme, 2005)

This author also suggests that an organisation even looking at Cybersecurity insurance as an educational exercise will get people thinking about security of data with greater focus, and therefore may start the process of counteracting the market failure. A number of other papers at that time reported more overtly on the same theme (Kasen et al, 2004, 2005).

The author of the paper quoted above also proposed a model for cyber liability pricing based on an assessment of actual security risks within the organisation. Whether this paper provided the precipitation framework, or whether it had become part of the zeitgeist, within a short space of time many cyber-liability products were being offered to businesses within the competitive market place of the US. However, assessment of the business for suitability for cyber liability insurance was time-consuming, and an automated assessment tool was sought to make the job a lot quicker and more efficient.

#### *Information Security Standards and Cyber-Liability Insurance*

All this had happened before the UK project which became known as IASME was anything beyond blue sky thinking, let alone commercially available as an alternative to ISO27001, ISF, ITIL, COBIT etc. The increasingly widespread availability of cyber liability insurance in the US brought about Bohme's predicted effect and helped to influence the status of ISO27001 in that country as insurers significantly reduced premiums for companies that had achieved this standard. In the mid-2000s, a number of research papers emerged that suggested the insurance could play a part in improving cyber security awareness. An excellent analysis of AIG's Net Advantage was undertaken by Bohme and a US based colleague at Carnegie-Mellon (Bohme & Kataria, 2006) and a proposal was made for enhancement with their suggestion of an "equilibrium model" to provide information for the cyber-insurance market. Particular types of business were identified as being most appropriate as early adopters for cyber-insurance. Judging by the subsequent success of AIG in the cybersecurity insurance market, it seems likely that the results of this academic collaboration were used wisely.

There is no doubt that US organisations today are much more “risk aware” now than hitherto, and much more prepared to spend to improve their information security. One reason for this change is cited as the progressive roll out of new laws (State of California, 2003; US Federal Government, 2002) and regulations (PCI Security Standards Council LLC, 2008), which have obviously increased awareness. Also, as a result of incidents within the US Defense supply chain (US Government, 2010) there has also been a change in requirements for US government and other supply chain contracts (WhiteHouse, 2011), and businesses have started to find that they are required to show evidence of insurance cover for information assets in order to get business. The growth of cyber liability insurance also contributed by making

information security a mainstream topic for conversation, a necessary precursor for information assurance to achieve acceptability in the SME market place.

### **Using Insurance to influence UK SME Cyber Security**

The research conducted on UK SMEs regarding information security is at least consistent. Most of them do not see it is a priority, and are therefore unlikely to spend on it, so market failure does seem an appropriate description. However, a small but significant minority are concerned about their information security, do worry about a data breach, and do see tightening up information security as one of their priorities looking forward.

The latter group is important because they can influence others by what they say and do. As previously stated, the mere act of getting cyber liability insurance into the marketplace raises its profile, and could make a difference to the zeitgeist. The UK does not benefit from powerful legislative drivers for business attitudes to change, and that leaves just the supply chain hubs and cyber liability insurance providers to act as the change agents. Of course the insurance companies could be regarded as supply chain hubs in their own right, so getting one of these on board is crucial. Thanks to the efforts of Duncan Sutcliffe, one of the companies involved in US research and roll out of cyber security product, AIG, became involved.

Sutcliffe has noticed that some business contracts in the UK are now requiring some sort of reassurance about protecting information assets and compensation in the event of a breach. Cyber liability insurance is an obvious way to provide that reassurance. Supply chain pressure often brings about change. A good example is the requirement in the construction industry for some kind of reassurance against data breach, and now all construction contracts include a clause about insurance cover. Other supply chain pressure is starting to emerge through public sector procurement requirements. Also, more lawyers have specific knowledge of the laws relating to data breaches and cyber security, and are starting to word contract requirements accordingly.

Also, there are recent signs (Holmes, 2013) that the continued concern about a lack of policing to catch e-criminals, and insurance seen as the next best thing for protecting assets. Cyber Liability Insurance is certainly becoming a matter for discussion, and this excellent recent article in a popular security monthly publication ably demonstrates (Sambhi, 2013), and such articles are likely to promote further discussion. Finally, the proposed tightening of EU Data Protection legislation, which will become EU Law in 2014 (Ashford, 2013), will cause a big rise in insurance to protect information assets. All of these factors are impinging on the business community at the same time, and creating the climate for a change of business attitudes.

#### *The Model*

An important part of any product marketing is to offer incentives to the buyer, and the insurance industry does this through offering reductions based

on a history of “good behaviour”. Car insurance premiums are lower for "good drivers". One measurement of being a "good driver" is a lack of recent accidents and consequent claims, and zero penalty points on the drivers licence. What constitutes good information management, and how can this be demonstrated? One way a business can do this is to by getting certified against a recognised and appropriate (for their business) information security standard. It was acknowledged, however, that UK SMEs would be very unlikely that would wish to become involved with a cyber security insurance product specifying ISO 27001, for reasons previously discussed. One new standard aimed at SMEs had recently emerged, however, and that was IASME (Henson et al, 2011).

Sutcliffe discussed possibilities for AIG involvement in the UK, where attitudes to cyber liability insurance had recently become more favourable. The cyber liability offering to businesses had been developed in the US over a number of years and was fairly comprehensive in terms of the protection it afforded. The assessment process for a business was based on a series of "self-check" information security questions, and the responses were taken in good faith by the insurance company to be correct. The areas that needed to be covered have also been refined over many years so that the range of protection covers typical business needs.

The possibly contentious area, at least as far as some security professionals is the use of self-assessment. If the business lies, and then gets breached, won't they get insurance under false pretences. The developers of IASME were firmly in this camp. Indeed, previous requests for a self-certification version of IASME had been resisted on grounds that an auditing model for assessment was the only safe basis for certification. However, as the IASME team discovered, insurance is different. It has been around a long time, since the early ships set out on voyages across the seven seas. Yes, some people do lie, but insurers are well aware of that. Where the "back end" of insurance infrastructure kicks in, is when the customer makes a claim. If any of the questions have been answered inaccurately (and robust checks are made!) the customer won't get their claim paid.

In cyber liability insurance, this is a safeguard for the assessment where the insurance model is concerned; the further process that comes into play if a claim is made will reveal the lies (or misunderstandings?) in any of the original responses given to get the insurance in the first place. If the responses are found not to be truthful the insurer reserves the right to withhold compensation. In the light of this new information, the IASME team agreed to reengineer IASME to be self-certified... but a "self-assessed" certificate would initially only be issued for insurance purposes!

AIG underwriters have looked closely at IASME compared to the 20 or more "tick box" questions they normally ask. A further advantage of IASME as opposed to a traditional tick-box approach is that information risk is an essential component of the process, and SMEs are required to scrutinise their existing systems or areas that could be considered as low, medium, or high risk. This is useful information for insurers, and can help the SME focus

resources most appropriately to achieve an acceptable overall area of risk that the insurer would be comfortable to insure.

#### *Engaging SMEs with the Model*

IASME have continually been asked for a simple, cheap self-assessment tool by small businesses, as a first stage towards developing their own ISMS, and the insurance model enabled this to happen, with the understanding that only self-certification provided was not the IASME-approved process, and could only be used for their own internal processes and for insurance purposes, which carried their own safeguards.

The opportunity to develop a self-certified version of IASME has led to a trial with some local SMEs, and the results so far have been encouraging. Once these have been appropriately evaluated, this service can be offered more broadly to SMEs, again with the proviso that the results are only used for internal purposes or for insurance purposes. IASME certification with the IASME badge is based on auditing, and the distinction needs to be clear. However, SMEs could otherwise be put off even applying for cyber liability insurance if they know there is to be a test of some kind, and the fact that there is a local standard coupled with the assessment process may reassure them, and encourage them to participate.

Apart from the potential attraction of IASME, the engagement (or not) of SMEs depends on the ability of AIG and rival insurers to create a market in an area that has rightly been associated with market failure. The AIG product was only launched in February 2013, and IASME itself is only used by a small number of SMEs. Both IASME and Cyber liability insurance are getting exposure in the media, and it is anticipated that there will at least be some interest from potential early adopters worried about their information assets and in need of a piece of mind. Of course, as previously stated, there are many good economic reasons for SMEs tightening up on security and once a market starts to emerge all these factors can be given an airing.

When one of the authors started out on this daunting journey to improve SME security, the words of Mahatma Gandhi came to mind:

“First they ignore you, then they ridicule you, then they fight you, and then you win.”

Plenty regarded the task of engaging SMEs with systematic and auditable information security as laughably difficult, but information assurance for SMEs does now seem to be in the serious phase, with UK government interest in offering something to SMEs as part of their Cyber Security Strategy (HMG, 2011).

#### *Effect on SME Attitudes to Information Security*

As already stated, it is early days for this new model! The IASME team have now been working for a number of years with SMEs with the goal of improving their security processes, and it has to be said that success to date has



been limited. Looking at the history of the growth of distributed computing, and the lack of education and understanding over many years at all levels, it is entirely understandable that SMEs think all is OK, and that the security horrors presented are mostly hype to get them to buy security products. In the absence of tighter legislation, a change in behaviour will only change with a change in attitude. There is evidence that availability of cyber liability insurance has influenced SME attitudes in the US, so it is not unreasonable to expect a similar effect in the UK.

The numbers of SMEs seeking certification via IASME or any of the other potential standards available to them will be carefully monitored. The last time such a survey was undertaken at University of Worcester, the results showed very little engagement with standards. A further survey in 2014, as cyber liability insurance becomes increasingly available at a competitive price. As already stated, there are suggestions that the impending change in the law will bring about an attitudinal change, although there is little evidence that previous changes had much effect, because of the perception that the law was not realistically policeable with the allocated resources. There is no indication from UK government that more resourcing will become available for enforcing the new law when it become statute, so this state of affairs seems set to continue.

Against this backdrop, with concern continuing to increase, insurance is certain to become a potential solution, as it has been for some against criminal activity against physical assets in the home. This will only start to influence attitudes as the market develops, and insurance companies are seen to be in direct competition to get SME business insuring their information assets. The existence of that competitive market will certainly cause businesses to talk about the subject because it will offer them (if the price is right...) an affordable solution. The suggestion so far (from the AIG product just launched in the UK) is that the price is competitive, and offers SMEs a wide range of safeguards for information assets. However, SMEs do not part with their money easily, and one suspects that there will be a slow, reluctant acceptance, and increased awareness coupled with enhanced legislation and supply chain requirements, will cause a shift in SME attitudes.

## **Conclusions**

In the US, Cyber Liability insurance has been effective in helping to raise awareness about organisational information security, and has created a lucrative market for the insurers. It is early days for this type of insurance in the UK; a product that works in the US does not necessarily work in the quite different culture of the UK. However, most UK insurers do seem to be looking at introducing their own products so it seems that changes are definitely underway. The progress of these new products is of interest to information security researchers because it opens up a new flank in creating a market for information security certification amongst small businesses.

As this paper is written, implementation of a cyber liability model for SMEs is in its infancy. The offer of insurance won't of course have much impact on those SMEs who don't worry about a data breach, let alone think about its costs. However, there is sufficient curiosity and response to create an interest and talking point; previously trying to get the average SME owner interested in information security was an almost impossible task. Through careful use of this model with motivated SMEs, it is to be hoped that a win-win scenario will follow, with information security awareness and actions dramatically improved, and a new market opened up for the insurers.

## References

- Acquisti et al, 2012, "Empirical Analysis of Data Breach Litigation", WEIS 2012, [online at [http://weis2012.econinfosec.org/papers/Romanosky\\_WEIS2012.pdf](http://weis2012.econinfosec.org/papers/Romanosky_WEIS2012.pdf)]
- Ashford, 2013, "Proposed EU data breach laws will require proactive security", Computer Weekly [online at <http://www.computerweekly.com/news/2240176411/Proposed-EU-data-breach-laws-will-require-proactive-security>]
- 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.
- Bohme R, 2005, "Cyber-Insurance Revisited", WEIS 2005, [online at: [http://wi-vm988.uni-muenster.de/security/publications/Boehme2005\\_CyberInsurance\\_Revisited\\_WEIS.pdf](http://wi-vm988.uni-muenster.de/security/publications/Boehme2005_CyberInsurance_Revisited_WEIS.pdf) ]
- Bohme R & Kataria G, 2006, WEIS 2006, "Models and Measures for Correlation in Cyber-Insurance"
- Detica, 2011, "The cost of Cyber-Crime", [online at [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/60942/THE-COST-OF-CYBER-CRIME-SUMMARY-FINAL.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60942/THE-COST-OF-CYBER-CRIME-SUMMARY-FINAL.pdf)]
- Gordon & Loeb, 2003, "A framework for using Insurance for Cyber-Risk Management",
- Henson, R. & Hallas, B, (2009) "*SMEs, Information Risk Management, and ROI*". In: Athens Institute for Education and Research (ATINER) SMEs Conference 2009, 10th-13th August 2009, Athens, Greece, [online at: <http://eprints.worc.ac.uk/958/>]
- Henson, R, Dresner D, & Booth, D, (2011), "IASME: Information Security Management Evolution for SMEs", Athens Institute for Education and Research (ATINER) SMEs Conference 2011, 1<sup>st</sup>-4th August 2011, Athens, Greece, [online at: <http://eprints.worc.ac.uk/1600> ]
- HMG, 1984, "The Data Protection Act".
- HMG, 2011, UK Cyber Security Strategy
- Holmes D, 2013, "Hacking threat and tougher data laws promise insurance boom", Reuters 2nd July 2013, [ online at <http://uk.reuters.com/article/2013/06/20/uk-europe-insurance-cyber-idUKBRE95J0CI20130620> ]
- ISMS, 2012, "International Register of ISMS Certificates, Register Search (Version 215 August 2012)"
- Kasen J P, Majuca P R, & Yurcik W K, 2004, "The Economic Case for Cyberinsurance", University of Illinois College of Law

- Law and Economics Working Papers [online at [http://www.queensu.ca/dms/DMS\\_Course\\_Materials\\_and\\_Outline/Readings-MPA831/Cyberinsurance-831.pdf](http://www.queensu.ca/dms/DMS_Course_Materials_and_Outline/Readings-MPA831/Cyberinsurance-831.pdf) ]
- Kasen J P, Majuca P R, & Yurcik W K, 2005, "Cyberinsurance as a Market-Based solution to the problem of Cybersecurity - A Case Study", WEIS 2005
- Lynn, William F. III, (2010), "Defending a New Domain - The Pentagon's Cyberstrategy"
- Moore, T, et al, 2012, WEIS 2012, [online at [http://weis2012.econinfosec.org/papers/Anderson\\_WEIS2012.pdf](http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf) ]
- PCI Security Standards Council LLC, 2008, "Navigating PCI DSS: Understanding the Intent of the Requirements".
- Siegel C, Sagalow T R & Serritella P, 2002, "Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security", Information Systems Security Volume 11, Issue 4, 2002, pp. 33-49
- State of California, 2003, "California Database Breach Act", [online at [http://info.sen.ca.gov/pub/01-02/bill/sen/sb\\_1351-1400/sb\\_1386\\_bill\\_20020212\\_introduced.pdf](http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020212_introduced.pdf)]
- US Federal Government, 2002, "The Sarbanes-Oxley Act"
- White House, 2011, "International Strategy for Cyberspace"