

An Investigation into the Current State of Information Security in the United Kingdom

Thomas Jackson^{1,2}, Daniel Fisher^{2,3} and Ray Dawson²

¹ Danwood Group, Lincoln, UK

² Loughborough University, Leicestershire, UK

³ ACNielsen, Headington, Oxford, UK

t.w.jackson@lboro.ac.uk

Abstract

The UK Government has set the target that by 2002, 25% of dealings by citizens and businesses with the Government should be able to be done electronically. The Government may have the technological and political framework in place to achieve this, but this investigation raises doubts about being able to instil a high enough level of trust within the UK population to achieve this goal.

Two questionnaires were designed to discover awareness of and attitudes to Internet security, one was sent to companies and one to existing and potential e-commerce customers. It was found that while companies had awareness of some aspects of IT security, awareness of trustmarks and other e-commerce security techniques was particularly low amongst small and medium sized companies. Adoption of company wide policies to protect their sensitive information is absent in all but the largest companies

Many of the public were also unaware of these security measures which lead to mistrust of e-commerce amongst the older population in particular. Awareness of the BS7799 Code of Practice and other similar guidelines and policies for companies was poor for smaller companies and the general public. The paper concludes that the overall findings indicate the current level of information security is inadequate within UK companies.

1 Introduction

The revolution of the Internet has had a great impact on the way that business is done, people communicate and information is shared. Today it is possible to order just about any product over the information superhighway, but the fear over security reduces the Internet's potential. In order to gain the conveniences that the Internet offers, e.g. the pages of the world-wide web, e-mail, and e-commerce, you have to forgo some loss of security. This loss of security results from hooking up to

a network, such as the Internet, which means there are more points from which a potential attack can be launched and there is a larger physical perimeter to protect. It is this balancing act between security and convenience that has led to the development of network security technologies and the creation of best practices and guidelines, in an attempt to provide consumers with the convenience of e-commerce while constantly maintaining an acceptable level of security.

There is always an enormous amount of press coverage following the report of a new virus, such as the recent Code Red II worm [1], the vandalism of a company's web site, or the success of a hacker accessing a company's network and stealing valuable private customer information. However this has led to the creation of uncertainty among consumers, whose fear of fraud and misuse of personal information has caused the slow up-take of e-commerce. According to the E-business review, online transactions accounted for only 2% of total sales in the UK in 2000, which was much lower than estimated (E-business review, July 2001).

Today there are just over 13 million active Internet users in the UK alone and over 236 million worldwide [5]. This paper investigates the current technologies and policies being used to create a secure environment in which to conduct business over the Internet. Particular attention has been given to, the technologies being used, the role of an information security policy, the Government sponsored British Standard for Information Security Management (BS7799) and the role of Trustmark schemes in e-commerce.

2 Data Collection

As this investigation involved discovering the current operating environment within UK companies, the initial step was to send an exploratory letter to a number of businesses in the hope that they would agree to participate in a short interview. However, due to the nature of this investigation and the current world-wide concerns regarding computer security, all of the companies contacted declined to take part in the research. This reply from British Airways was a typical response, "I regret it is our policy not to release details of our security measures into the public domain. I appreciate that this will be a disappointment for you but I hope you understand why this is necessary".

In an attempt to give companies more control over the amount and type of information that they could disclose, the approach was changed from that of an interview to a written questionnaire. This time 820 companies were contacted requesting their assistance with the questionnaire. The reply was more favourable, producing a large enough sample base to allow the questionnaire to be developed.

The questionnaire was created using Frederic D'Astous (2000) Guidelines. The initial stages involved what D'Astous calls, "a review of papers" [2]. This entails an analysis of current documentary sources ranging from web sites, newspaper articles and books to actually speaking with current experts in the field, to provide

a better idea of what has been said or written about the subject. This also allows for a better comprehension of the data once it is collected.

The next stage involved formulating appropriate questions in order to provide relevant data for the research. This helped to ensure that interesting but irrelevant questions were excluded, keeping the length of the questionnaire to a minimum in an attempt to keep the respondent interested. The questions were grouped according to subject type, with the more sensitive questions placed towards the end of the questionnaire. This was done intentionally to try to extract as much information as possible from the respondent. If the respondent sees a question at the beginning of the questionnaire that they do not want to answer, then they may decide not to complete the questionnaire. If the sensitive questions are towards the end of the questionnaire then at least some information has been generated, even if the questionnaire is incomplete. It was for this reason that information regarding the companies' security policy and use of technology was not requested until late in the questionnaire. As the questionnaire was sent by e-mail (as an attachment) or by post to the participating companies, it was important to initially re-inform the respondent as to the reason for the survey. This was achieved with a short letter. It was hoped that this would help to produce more informative data, as the respondent would know the type of information being requested.

A second questionnaire was designed to extract information from the public. This public questionnaire was developed along the same lines and was either sent by e-mail (as an attachment) to the respondent or was completed by hand in a face-to-face interview.

Both questionnaires were subjected to a pre-test to ensure that the questions were understandable and that the filter questions directed the respondents to the desired sections. This also helped to estimate the time needed by the respondents to complete the questionnaire and confirm that the hyperlink to the e-mail reply address was working and that the accompanying instructions were clear.

2.1 Demographics

The public questionnaire consisted of a 5-minute quantitative survey with a total sample population of 105 respondents (85 male and 20 female). The most frequent age group was the 20-24 year old range with 71% of responses.

The company questionnaire was again a quantitative survey, which lasted between 5 and 10 minutes. A total of 820 companies were approached randomly through the use of an online business directory and a sample population of 50 was created from those businesses that agreed to participate. The sample included 24 micro companies, 14 small, 10 medium and 2 large companies. 32% of the companies came from the wholesale, retail, catering and travel sectors, 26% worked in computing or other business services and 24% worked in finance or insurance.

Out of the total responses, 34% were from either the managing director, the proprietor or senior level management in charge of security, and a further 26%

were partners in the business. This was particularly the case amongst the smaller establishments, where 75% of the respondents from micro and small companies were either a partner or the owner. In the medium sized organisations the respondents generally had a specific responsibility for IT or risk, or belonged to the sales or marketing departments.

3 The Company Results and Analysis

3.1 Awareness of Industry Standards

Part of the company questionnaire was designed to discover what is happening within the smaller and medium sized companies in terms of their awareness of industry standards on security and their ability to implement the standards. As according to the DTI, the Government sponsored British Standard for Information Security Management (BS7799) can be used by “any size of business, in any sector, with any type of information systems, both manual and computerised”. It is therefore surprising that 94% of companies had not even heard of it and not one single company had achieved accreditation of the BS7799 standard. Of the 3 companies that were aware of the standard, 2 of them had no plans to adopt it within the next year and the third company was only considering applying for the standard. Reasons given for not attempting to adopt the standard included, “it is too costly”, “it is too time consuming” and “the business benefits of adopting the standard are not clear”. However, one company did have accreditation with a different standard, the ISO 9001 TickIT (the international standard for a Quality Management System).

This survey is not alone in discovering that not many companies have heard of the BS7799. The ISBS (2000) survey interviewed 1000 companies discovered that only 20% knew of the existence of the BS7799 and only 6% were able to quote the correct number [4]. The survey reported that awareness rose with company size, which is the reason for the difference in findings between this survey and the ISBS 2000 survey. However, the ISBS survey does support the authors’ findings in that less than 1% of companies were accredited with the standard.

The fact that the BS7799 standard is so complex and detailed has obviously helped contribute to the low adoption levels (although the poor awareness of the standard is the key reason). It is important that the security measures are of the highest standard but there is a requirement to make the standards achievable for even the smallest companies or even to invent a modified version of the standard for small to medium sized enterprises (SMEs). A less complex policy for SMEs would not provide the same level of security as the full standard but would give the smaller companies something to aim for and cause them to consider information security.

Figure 1 shows that with the exception of the Data Protection Act (probably due to the recent concerns over privacy of personal information and the large amount of press coverage which accompanied it), overall awareness of legislation and recommended policies is extremely low. It would appear that the companies aware

of one policy tend to be well informed regarding the others. All the companies who knew of the Common Criteria also recognised the C:Cure and UK ITSEC policies. This would suggest that these companies have an internal policy to ensure they are aware of all the latest guidelines. It is also apparent that awareness increases with company size. Out of the three companies aware of the standards in Figure 1, two of them were large companies and the third was medium sized. This could signal that SMEs are not being targeted or the targeting by the policy makers is ineffective.

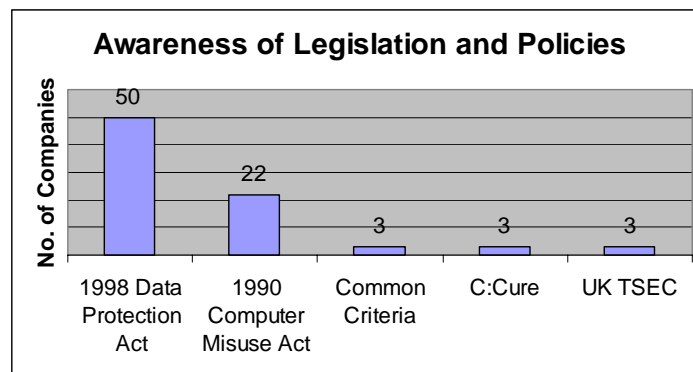


Figure 1 – (Q5) The Companies awareness of Legislation and Policies

Only 7 companies (14%) belonged to any type of online trust scheme, although 2 companies were in the process of applying for membership. Yet 82% of companies believed that such schemes help to increase customer confidence in e-commerce. It would therefore appear that the companies recognise the advantages that these schemes can bring, but are either unaware of them or are unable to meet the criteria. The fact that only 14% of the companies interviewed are members of a trust scheme would seem to show that awareness of such schemes are low and again indicates poor marketing on behalf of the scheme providers but also by the government. This poor awareness is illustrated by the companies' response (Figure 5) that more online trust schemes would help to decrease consumers security concerns. The fact that there are already at least a dozen such schemes indicates that many of them are not reaching their intended targets. The poor membership of trust schemes can also be explained by the fact that the advantage of belonging to a scheme is not as great as would be expected. It is clear that these schemes will only work if they create trust among consumers and encourage online purchasing. The public questionnaire shows that these schemes will work as 87% of respondents said that they would be more likely to buy online from a company accredited to one of these schemes. It also shows that the public are mostly unaware of them (only 41% of respondents were actually aware that such schemes existed).

Not all consumers believed that these schemes would motivate them to purchase online. Some admitted that they would still have security concerns (these will

probably never disappear completely) while others preferred to purchase goods in a shop where they could touch the products and interact with other people.

The following quote shows the concerns of a typical respondent considering online purchases and why this should be the driving force behind the creation and promotion of trustmark schemes: “I am happy with the current system as long as I use firms I have heard of”

3.2 The Policy behind Securing Company Information

The data collected shows that 80% of companies possess information that is considered either sensitive or critical in nature and 70% believe that information security is an important business issue. However, smaller companies do not share the enthusiasm for a formal information security policy that is advocated so strongly in the majority of e-business literature. In fact, fewer than half (44%) the companies interviewed actually had a formal policy in place.

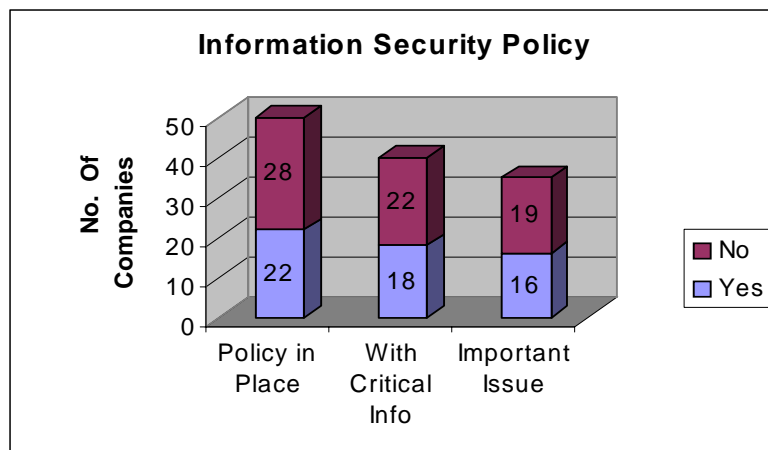


Figure 2 – Number of Companies with a Formal Information Security Policy

Figure 2 details the number of companies with a formal information security policy and shows the value they place on their information. Figure 2 shows that among the companies who admit to possessing critical or sensitive information, 22 of them (55%) do not have an information security policy in place. Within those businesses where information security is considered important only 46% (16 companies) have a policy.

It seems apparent that information is a valued asset and it is also clear that protecting that information is an important business issue even for these smaller companies. This is highlighted through some of the remarks received from the question “is information security an important business issue?”:

- “Customer information is the most important part of any business”
- “People must be confident their personal details are not available to unauthorised personnel”
- “It is important for me to keep my customers details secure as areas such as their security systems in place are discussed in my reports”
- “For customer confidence, if I hold information on my PC about customers, I would not like it getting into the wrong hands”

However given these remarks two of the companies quoted above have no information security policy. These companies value information as much as any other, however, either the knowledge regarding information security is lacking or the belief is that technology alone will suffice. Either way, the information and advice being provided by the DTI and other leading bodies is not disseminating through to the smaller companies who have the potential to destroy e-customer confidence just as much as the large companies. This point can be reinforced with a final quote from one of the respondent companies who believe that their data is safe if it is not on the web.

- “Information security is an important business issue but not for us. My organisation obviously contains information critical to itself...but it is not on our web site”.

All of the 50 companies interviewed had access to the Internet, although not all employees were privilege to that access. The majority of companies (62%) allow all of their employees access to the Internet and 41 companies allow at least 50% of their employees access. Only 18 companies (36%) have any sort of policy in place to regulate usage. This decreases to only 9 companies (29%) out of the 31 who allow all employees access. Out of the 16 micro-companies, all of them permitted employee access to the Internet with no policy in place, which perhaps is due to the micro-companies trusting their employees and being able to supervise them more closely should it be required. However, 22 companies reported that they had a formal information security policy in place and yet only 18 of them have a policy to regulate Internet use. This means that 18% of companies who have taken the time to implement a security policy are not covering one of their biggest threats, the Internet.

3.3 Awareness of Different Security Technologies

One of the questions that the company questionnaire asked was about the technologies the company had in place to secure their electronic information. It had already been established that all the companies had their own Internet web site and they were asked to indicate the type of technologies they were using, from a list of eight. The technologies were, Firewalls, Intrusion detection systems (IDS),

Passwords, Other login devices, Virus control, Data encryption, Virtual Private Networks (VPN) or Other and the results are shown in Figure 3.

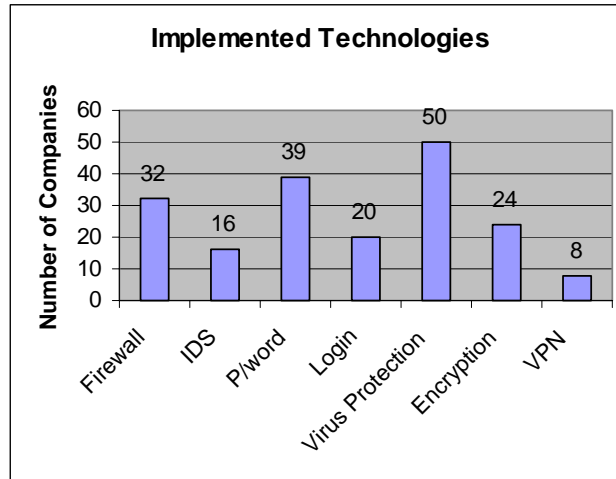


Figure 3 – The technologies implemented by the companies surveyed

It is interesting to note that every company interviewed said they had some form of virus control in place. Virus protection is probably one of the cheapest technologies in use to protect information, so it is not surprising that it is so popular. However, as with all technology, the product is only as effective as the management of it and anti-virus software needs to be constantly updated. The same applies to passwords, 78% of companies interviewed used passwords but they only provide security if they are accompanied by a security policy, detailing the minimum length of the password and advocating a mixture of upper and lower case characters. The use of passwords is noticeably less common among very small businesses, with 38% of micro companies having no password protection. This is probably due to a high level of trust, as there are fewer employees and probably even fewer computers.

It is quite surprising to see that 64% of companies are reporting the use of firewalls. Firewalls are considered the first line of defence in protecting private information but until recently have been rarely used by many companies. The Information Security Breaches Survey 2000 by the DTI reported that 82% of companies with external electronic links did not have any firewall protection however the findings from this investigation show that more companies are using what is quite sophisticated technology. One reason for this could be that, “firewalls today are low-cost and easy to deploy”, making them a more viable option for the smaller company with limited financial resources and technical know-how [6].

The other technological devices were included to see how advanced these smaller companies were, and it was not really expected that many of them would in fact use intrusion detection systems (32%) or other login devices (40%). The authors

felt that the company size and the accompanying limited risks would make the use of such technology inefficient. VPNs were also seen primarily as a tool for the larger companies, as a means to link remote users and branch offices. However, although only 8 companies reported the use of VPNs, it is interesting to note that 4 of them were micro companies with less than 9 employees.

The company questionnaire posed the question about the use of Public Key Infrastructures (PKI) within companies. The author's wanted to discover whether companies use PKI and if they were aware of future technological advances and the advantages or disadvantages that they offered to the company. It is obvious from the results that PKI is not in wide spread use at the moment, as only 2 of the companies interviewed presently use PKI (both of them have between 50-249 employees). This result is not surprising, however what is quite concerning is that 74% of respondents had not even heard of PKI. This is a technology which is seen as the saviour of e-commerce, and yet three-quarters of companies have no idea what it is. One respondent best described the advantages of PKI as "debatable" while the main drawbacks described as:

- a lack of interoperability between vendor products (14%)
- a lack of knowledge/in-house experience of PKI (10%)
- the cost involved (10%).

Showing again that, although the technology might be in place to enable PKI, the knowledge and resources among businesses are certainly not.

4 The Public View of Information Security

The public questionnaire was designed to discover what the Internet using public thought about the current level of security on the Internet and to investigate if the public understand the technology being used by e-commerce companies. Another facet of the investigation was to establish if the current level of technical security within companies is making a difference with the customers as far as Internet purchases are concerned.

The results show that 74% of respondents had used the Internet to purchase goods or services but less than half of them (42%) were concerned about giving out their credit card details, which may indicate an understanding of the technology and thus, the high level of security on the Internet. Of those with concerns, the main worries were fraud (82%) and not being absolutely sure about the level of security on the web site (12%).

Figure 4 shows the responses that the customers gave for not being concerned when making Internet purchases. A total of 45 customers were not concerned about providing credit card details.

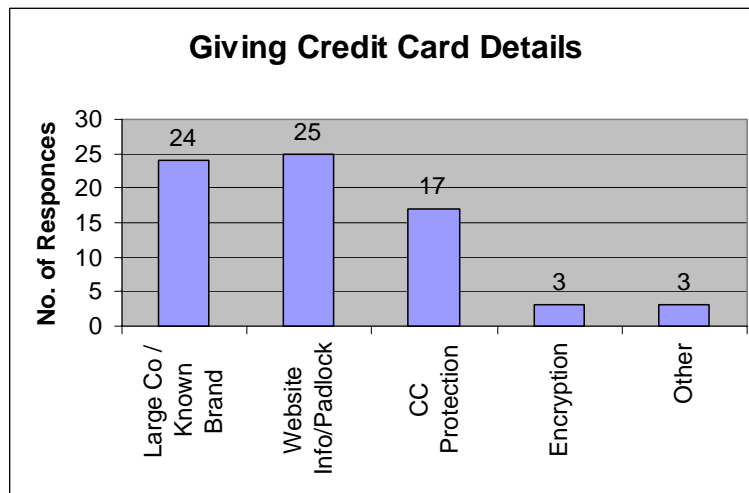


Figure 4 – Reasons for not being worried about giving out credit card details
(Please note, the respondents could provide multiple answers)

Figure 4 shows that customers feel more secure when buying from a large company with a well-known brand (56%). This is understandable, as most large companies also have a high street presence which gives the customer added reassurance when it comes to remuneration or any problems.

Customers also feel reassured (53%) by the padlock symbol (indicating a secure connection) and by the information on the company's web site regarding technology and their privacy policy. This shows an understanding of the technology being used and a trust in the company, which is the reason for the inclusion of the technological and privacy policy information on the web site. Thirty-eight percent of the customers recognise the protection that credit cards offer to the online purchaser and 7% trust the use of encryption technology to secure their transactions.

While 42% of respondents were concerned about purchasing online, only one respondent claimed to have been the victim of any type of Internet crime. This helps to prove that most of the concerns surrounding the Internet and its security are in fact unfounded and merely a product of intense press coverage and a lack of understanding of the technology. Sixty-three percent of the respondents, who had not purchased anything over the Internet, cited financial security as the main reason. This indicates that although many people use the Internet frequently to purchase goods, it is those people who have never used the Internet that fear poor security the most. It is interesting to note that the average age of the respondents who have never purchased over the Internet is 31 years of age. This is a difference of just over 7 years when compared with the average age of those who have purchased over the Internet (23.8 years old). It is a clear indication that the Internet is being understood and used by the younger generations, who have grown up in

the Information Age. This can only be good for the future of the Internet and is a clear sign that the technology being used by businesses and the messages they are sending out to customers is helping to remove many of the preconceived concerns that surrounded the Internet for so long.

To further enforce this point, the second most common reason for not buying over the Internet, was that the customer had not found anything to buy (48%) and had nothing to do with security or not understanding the Internet. Concerns regarding the delivery of goods (30%) and the problems regarding returns and refunds (33%) were also mentioned.

The final question in the security section was designed to discover the public's attitude towards a technology, aimed at limiting fraudulent use of credit cards. The introduction of pre-paid, unique numbered cards with a limited value would keep any loss sustained to a minimum. It would ensure that even if someone did illegally get hold of your card details then the most they would be able to extract from it would be the maximum value of the card (say £50) and not the entire contents of your bank account. These cards (similar to mobile phone top-up cards) are designed to limit fraudulent use rather than overcome it and would be, aimed at the lucrative youth and teenage markets [3]. Sixty percent of respondents indicated that they would prefer to use these cards rather than their credit card. This figure rises when those who have not purchased over the Internet are asked, as 78% of them would prefer to use these cards. Indicating again the high security concerns among those consumers who have not yet used the Internet and highlighting the need for more information and education about the Internet.

5 Improving Security and Confidence on the Internet

To understand how security could be improved and how the confidence of using the Internet could be increased, the public and the company questionnaire asked the question how this could be done. Figure 5 shows the replies to questions from the public and company questionnaires respectively.

Forty-seven of the respondents had no idea what could be done to increase confidence, indicating the lack of awareness and knowledge about the Internet in general. However, 50 respondents believed that trust schemes would help to achieve both security and confidence if they and their details were promoted more, so that more people knew about them.

Experience of the Internet (as more people have access to and understanding of it) and more training and education about the Internet and its workings i.e. what to look for in a secure site, was mentioned by 25 respondents. Once again showing how vital it is that correct information regarding Internet technologies and policies are targeted more effectively and more vigorously.

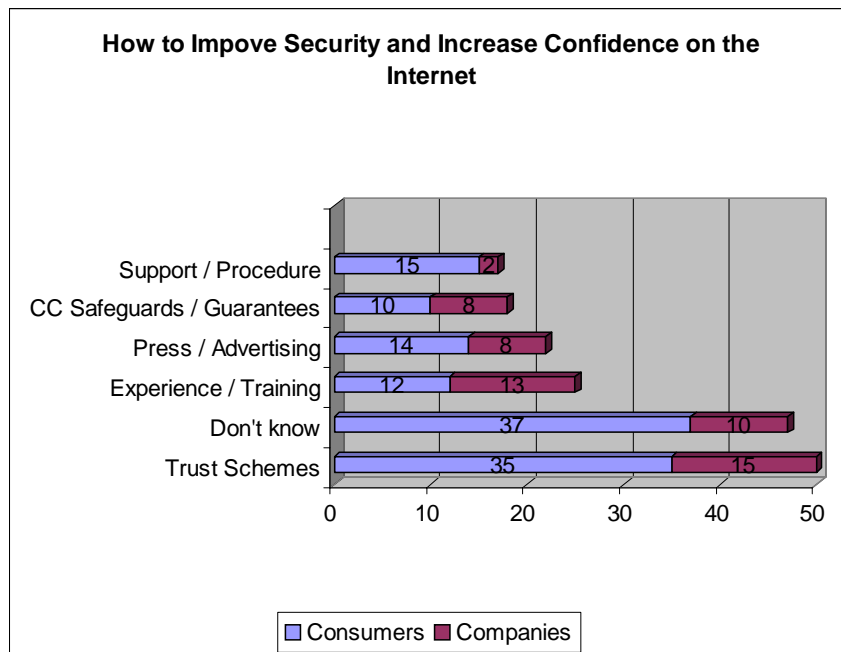


Figure 5 – What Companies and the Public believe can be done to Improve Security and Increase Confidence on the Internet.

The media was blamed in some way by 22 respondents, either because of the hype surrounding poor Internet security and the focus on horror stories rather than the successes, or because of the lack of advertising on television by online companies and poor information about technology when they are advertised.

Finally, 17 respondents recommended improved customer support from companies, in the form of

- Availability of contact details, phone numbers and telephones that are actually answered by a human rather than a machine
- Better delivery (both faster and only to the address of the credit cardholder)
- Alternative methods of payment (like telephone or post) to reduce worries over credit card details being stolen.

This demonstrates the fear and lack of knowledge surrounding Internet security, as credit card details are more likely to be stolen by a thief in a restaurant or shop as they are being swiped through the machine than over the Internet. Credit card losses on the Internet rose from £2m to £7m last year, however the rate was slower than for all other types of card fraud (E-Business Review, April 2001). It is the press reports and the fact that the Internet is new and has become popular so quickly that mean consumers are going to be apprehensive about using the Internet

until more information is provided for them. The information is available but it must be directed at the consumers rather than merely being there for them to read should they wish. If e-commerce is to flourish then it needs to become more transparent with information about technology and policies and practices. The bad press needs to be balanced out with good reports and informative adverts and the current range of literature and guides (particularly those aimed at SMEs by governmental bodies) need to be more readily available.

6 Conclusion

The UK Government has set the target that by 2002, 25% of dealings by citizens and businesses with the Government should be able to be done electronically. This is intended to lead the way and encourage the expansion of e-commerce within the UK as a means to decrease the costs for new businesses to enter new markets and create greater efficiency within the economy. The Government may have the technological and political framework in place but this investigation raises doubts about being able to instil a high enough level of trust within the UK population to achieve this goal.

The Internet is meant to be a business enabler, breaking down the costs of entry into markets and allowing smaller companies to reach a bigger market. It is the role of the Government, in the shape of the Department of Trade and Industry and other bodies, to provide the SMEs with the information they require to use the necessary technologies and to implement the latest policies. Not just because they want the SMEs to compete but also because the Internet is seen as the future of business. By creating a secure operating environment now and having consumer confidence in e-commerce improve, the Government is aiming for a more prosperous economy in the future. So it is vital that the SMEs are at least made aware of the latest information security policies and technologies in order to decrease the number of security breaches on the Internet and increase the level of consumer confidence.

This investigation has shown that the larger companies tend to have all the recommended equipment in place to safeguard their information and this is consistent with the degree of risk and potential loss that these companies face. It was expected that the SMEs would not employ the same level of technology but, in fact, the use of technology was higher than anticipated with almost half of all companies interviewed using firewalls, password controls, virus controls and encryption. This would indicate that companies are aware of the need for Internet security and understand some aspects of the current technology. However, future technologies like PKI and m-commerce were not widely adopted and almost all respondents were totally unaware of their potential, indicating that technology is advancing quicker than the SMEs can keep up with. It has been outlined in this paper that continual reappraisal of technology and practice is necessary to keep information secure and this could indicate a future threat to SMEs, as hackers become more sophisticated, companies could remain stagnant.

Information security, and particularly the BS7799 code of practice for information security management, is not really present within SMEs, despite the attempts by the DTI to involve these smaller enterprises. Companies appear to be mindful of the value of information but seem to be unaware that anything can be done to protect it.

This is not specific to the BS7799 as there seems to be a poor awareness level for the majority of policy and best practice guides. There appears to be a fundamental fault somewhere in the system, which is meaning that information written specifically for SMEs is not getting through to them. This is information that is vital for the future of the Internet, as it will help to create a more secure environment and release the full potential of the Internet. Of those companies that do have an information security policy in place, very few of them appear to be detailed enough to actually enhance information security.

To conclude, the overall findings indicate that the current level of information security is inadequate within UK companies. IT security appears to be in place but the adoption of a company wide policy to protect the information is absent in all but the largest companies. Companies with the most to lose, who have built up a reputation perhaps away from e-commerce and are now entering the Internet, are not prepared to risk everything they have worked for by implementing sub standard information security practices. The smaller companies, on the other hand, with no real financial or legal incentive to implement best practices, are making very little effort to become aware of their existence. This is likely to continue until SMEs are forced to do otherwise through some form of legislation.

7 Bibliography

1. CERT. "Security Practices and Evaluation", www.cert.org, 09 September 2001
2. D'Astous, F. "Guide to Questionnaire and Surveys", www.members.tripod.com/frede_dats/conseill_a.html, 2000
3. Duffield, C., "Securing trust for transactions". E-Business Review. February 2001, Vol 2, Issue 2.
4. ISBS. "Information Security Breaches Survey", 2000.
5. Nielsen, "Who are We", www.nielsen-netratings.com, 2000
6. Oxley, P., "The Requirement for Firewalls in the 21st Century", www.wickhill.co.uk, 2001