Published in Internet Research, *Internet Research*, vol. 9, no. 5: 372-382 1999

Security implications of Electronic Commerce: A Survey of Consumers and Businesses

S.M.Furnell and T.Karweni

Network Research Group, School of Electronic, Communication and Electrical Engineering, University of Plymouth, Plymouth , United Kingdom

e-mail : sfurnell@plymouth.ac.uk

ABSTRACT

Electronic commerce is poised to become one of the major applications areas in the Internet / World Wide Web environment, with significant growth forecast to occur within the next two to three years. However, one of the significant requirements for the success of e-commerce is trust, on the part of both the consumers and businesses offering services. It can be observed that while e-commerce services are now being offered on the Internet, a number of examples can be cited that suggest sufficient protection has not been fully achieved.

The paper examines the general requirement for security technologies in order to provide a basis for trust in the e-commerce environment. The discussion is supported by the findings from two surveys, conducted by the authors, among general Internet users (i.e. potential target consumers) and commercial businesses. These surveys considered both the attitudes to e-commerce in general and opinions relating to the associated security requirements. Attempts were also made to assess the respondent's knowledge of the existing security safeguards that may be applied.

The survey results suggest that, while there is significant concern amongst Internet-based consumers regarding the security of their purchasing activities, these are outweighed by the merits offered by the medium. The results also suggested a lack of awareness or understanding of the security technologies that are available and it is concluded that overcoming this problem would help to establish a wider foundation of trust in the new technology.

KEYWORDS

Electronic commerce, security, consumer attitudes, business attitudes.

Published in Internet Research, *Internet Research*, vol. 9, no. 5: 372-382 1999

INTRODUCTION

Recent years have seen an explosion of activity in the domain of electronic commerce (e-commerce). Interest in the concept, and its predicted impact, is such that it has become more than just a current buzzword within the IT industry. Indeed, the issue has become the focus of significant mass media interest.

The concept of electronic commerce can be defined as (DTI, 1999):

> "using an electronic network to simplify and speed up all stages of the business process, from design and making to buying, selling and delivering"

It may be argued that e-commerce is not a new phenomenon, with related activities such as Electronic Data Interchange (EDI) having occurred since the 1970s (Chelmsford, 1999). However, this referred to essentially business-to-business transactions, operating within a closed environment. The difference now is the use of the Internet as an enabling technology, making e-commerce services directly accessible to the average person. Such business-to-consumer e-commerce, and the associated security issues, represents the particular focus of this paper.

Businesses communicate with customers and partners through many channels, but the Internet is one of the newest and, for many purposes, best business communications channel. It is fast, reasonably reliable, inexpensive, and universally accessible. It reaches virtually every major business and more than 100 million consumers from all over the world. There are around three million traders on the Internet today. According to predictions such as those by Ameritrade Holding Corporation, this figure will to rise to 14.4 million by 2002. Until recently, the traditional presence of businesses on the WWW could be analogised to a "shop window" approach - where you can see what products or services are available, but you cannot actually purchase them directly. This is now changing and the web is being put to more varied uses with sites such as Amazon.com (online bookstore) and eBay.com (online auctions). Such populist uses may well be the catalyst for getting more people to buy online. In 1996, Internet purchases totalled $500 million. This is forecast to increase to $1 trillion by the millennium (Howell, 1998).

As the paradigm shifts from "browse" to "buy", there is an increasing requirement for data security and protection of systems within the scenario. These issues are discussed in the next section, leading to a survey of current attitudes towards e-commerce and its associated security.

BARRIERS TO E-COMMERCE ADOPTION

In order for the Internet to be accepted as a viable platform for e-commerce it is necessary to establish a foundation of trust amongst the participants. Trust is, of course, also important in the context of traditional commerce and has been developed over time through the formation of

appropriate policies, procedures and practices to safeguard transactions and company assets. However, a comparable safety net is not yet fully established for electronic commerce over the Internet. Furthermore, because of the global nature of the Internet as a public network, the issue of trust has even greater importance than in traditional commerce because:

- the party being dealt with may be unknown;
- it is not possible to have full control of the data during its transfer (for this reason, some people use the web to locate products but prefer to place their order via telephone or fax);
- the other party might be at different and unknown physical location and, therefore, might have different rules and legislation

Ratnasingham (1998) states that it is necessary to facilitate a "complete trustworthy relationship" amongst the trading partners within this context. In order to achieve this, a number of requirements must be satisfied:

- if the other party is not known directly, then there needs to be the additional involvement of a someone else known to both sides (i.e. a third party who can be trusted);
- data needs to be secured at all stages;
- common rules need to be established or, failing that, at least a known and acceptable (conducive) legal environment.

In respect of the second point, the security requirements associated with different stages of an e-commerce relationship are illustrated in table I.

Requirement	**Typical considerations**
Security at the user side	– Physical access control to the machine – User authentication and authorisation
Security during transport of data	– Confidentiality – Data integrity
Security at the merchant side	– Secure storage of user information – User's privacy protection – Authentication of parties involved

Table I: E-commerce security issues

These requirements have already been recognised within the Internet / e-commerce community and a number of technologies exist that may be used to satisfy different elements. The most common approach used to secure current online transactions is the Secure Sockets Layer (SSL) protocol developed by Netscape (Frier et al. 1996), which allows encryption of messages, message integrity and authentication services to be provided. SSL consists of

Handshake and *Record* protocols. During the handshake stage, the client and server systems exchange messages to negotiate security enhancements during the initiation of a TCP/IP connection. The result of this handshake is that the client and server agree on the level of security to use and a set of algorithms for privacy and authentication. Once the connection is established, the SSL record protocol can be used to transfer all data in encrypted form. SSL is independent of the higher level application and was designed to provide security in a variety of scenarios (i.e. not just in an e-commerce context). Version 3 of SSL has been used as the basis for a new protocol, Transport Layer Security (TLS), which shares the property of application independence but is being developed as a non-proprietary approach (Dierks and Allen, 1999).

An alternative to the SSL/TLS approach, and one which has been specifically devised with online e-commerce transactions in mind, is the Secure Electronic Transaction (SET) standard developed by the major credit card companies (SETCo, 1997). SET is published as open specification and applicable to any payment service. It addresses several security needs specific to electronic commerce:

- privacy of payment data and confidentiality of order information transmission;
- authentication of a cardholder for a branded bankcard account using digital signature and cardholder certificate;
- authentication of the merchant to accept credit card payments using digital signature and merchant certificate;
- payment information integrity is ensured by the use of digital signature;
- special purpose certificates;
- non-repudiation for dispute resolution.

The significance of SET over other Internet security protocols is the use of Digital Certificates (X.509 version 3) that associate the cardholder and merchant with a financial institution and the Visa and Master Card payment system. The use of this digital certificate will prevent a level of fraud that the existing systems do not have and gives the cardholders and merchant confidence that the transaction will be handled with the same manner as credit card transaction handling today.

While such technologies are clearly necessary, they do not represent a complete resolution of the trust issue. Indeed, if examined from a critical perspective, there is still substantial evidence to suggest that trust is not yet warranted. For example, there have been publicised discoveries of weaknesses in underlying e-commerce technologies that were previously claimed to be secure. An example here relates to the identification of a flaw (which has since been addressed) in the SSL approach, which could allow unauthorised decryption of messages (Bicknell 1998). While analogies could be made here to the illicit exploitation of previously unrecognised "loopholes" in traditional trading systems, the difference is that the public lacks a basis for trust in electronic systems from the outset and, therefore, require proof of its security before being willing to use it. By contrast, because the operation of a traditional trading system is relatively

transparent, we are sufficiently satisfied that we understand the basic mechanisms at work and are, therefore, willing to place our trust in it.

Another example of the need to establish trust is the experience of the credit card operator VISA in relation to Internet-based transactions and instances of fraud. While only around 2% of their credit card transactions are currently conducted via the Internet, this accounts for about 50% of disputes and discovered frauds (Hancock, 1999). The publication of such statistics is unlikely to improve public confidence in e-commerce or the Internet environment in general. In addition, there is a lack of harmonised legislation in the field. As a consequence, there is no significant practical experience within the legal system and/or case law that may be used for reference in settling disputes.

Despite the problems highlighted above, there is clear evidence to suggest that business-to-consumer e-commerce is on the increase. As such, the questions arise of what factors are driving this adoption and whether the consumers and businesses involved are aware of or concerned about security issues. The authors have sought to investigate these issues via surveys conducted amongst individual Internet users and commercial organisations offering (or considering) e-commerce services.

A SURVEY OF CONSUMERS

Background and procedure

The first survey was conducted amongst individual members of the general public. The overall objective of the exercise was to determine people's attitudes, awareness and expectations in term of security in an e-commerce environment.

A questionnaire was developed that included a total of 16 questions, all of which required tick box responses (and, in some cases, brief written answers if a box such as 'Other - please specify' was ticked). Questions 1 to 8 were used to determine the respondent's background in term of age, education, credit card ownership and computer / Internet usage. Questions 9 to 11 attempted to assess the respondent's willingness and reasons for purchasing online and whether their attitudes are related to concerns and/or awareness of security issues. Finally, questions 12 to 16 were intended to determine the respondent's opinion on aspects such as credit card usage and other online payment technologies, and general expectations of security and privacy.

A total of 100 questionnaires were distributed in paper form (to members of the public in the local area), along with an online version that was made available and publicised on the authors' WWW site (see http://ted.see.plym.ac.uk/ecommerce). This yielded a total of 38 responses to paper surveys and 26 online results. This final total (i.e. 64 responses) was considered sufficient to at least gain a general appreciation of end user / consumer opinions.

Results

The vast majority (83%) of respondents were male. In terms of age, 45% were aged between 16 and 24, 51% between 25 and 39, and the remainder 40 or over. The respondents generally appeared to be IT literate, with 61% claiming to use a computer both at work and at home. 45% claimed to use a computer for between one and four hours per day, while a further 36% claimed up to eight hours use and 14% claimed over eight hours. Only two respondents claimed to use a computer for less than one hour per day. Over 90% of the respondents were Internet users and examples of their usage are indicated in table II below.

Reason for use	**Home**	**Work**
Email	52%	91%
Search for product information	47%	73%
Shopping or purchasing goods	22%	30%
Downloading software	52%	64%
Search for information	50%	84%

Table II: Examples of Internet usage

The conclusion drawn from this was that most of the respondents are potential candidates to be electronic commerce users. Later questions would establish the degree to which this was the case.

Given that it currently represents the primary mechanism for online purchasing, the respondents were asked whether they owned a credit or debit card, of which 86% replied affirmatively. Of these, 47% claimed to have already used it for an Internet-based transaction, which was considered to be a fairly significant proportion and, again, indicates the general IT literacy of the sample group.

The full set of respondents was asked whether or not they had purchased online and were asked to indicate their reason(s) why. A total of 42% claimed to have purchased online, with the main reason being the attractiveness of the offer (55.5% of cases). In addition, 85% of respondents who had purchased online also cited some other reason. These included fast response from the retailer, access to international shopping and a wider range of products, and that online purchase was the only option available to them. Of the 58% who had not yet purchased online, the main reasons were concerns over insecure communications (51%), potential untrustworthiness of the vendor (43%) and no need to buy online (46%). These results suggest that the issues of trust and security are currently preventing a significant proportion of individuals from becoming involved in e-commerce activity.

The respondents were also asked whether they had any concerns about doing business via the Internet. While a small proportion (11%) claimed to have no concern, the majority of respondents cited at least one concern. The biggest problem was perceived to be communications security, cited by 61% of respondents. Use of personal information by the vendor (55%), vendor authentication and credibility (52%) and vulnerability of the vendor's internal network (33%) were other suggested concerns. The fact that the figures relating to communications security and vendor credibility are higher than the corresponding figures from the previous paragraph suggests that a proportion of the respondents who *are* currently purchasing online are doing so in spite of their concerns.

Given that concerns were expressed, it was also interesting to determine whether the respondents were aware of the security technologies that might be used to combat them. A number of e-commerce related security technologies were cited and the respondents were asked to indicate their awareness of them (all of the technologies chosen are, to some degree, known to have been mentioned in mass media newspaper articles). Table III summarises the results observed. It should be noted, of course, that the respondents' interpretation or level of understanding of these technologies was likely to be quite variable. The authors were particularly surprised to see 50% of the respondents indicating a familiarity with the concept of certification authorities, while only 33% were aware of the related issue of Trusted Third Parties. As such, the validity of this particular result is questionable and it is assumed that many respondents had an incorrect interpretation of the term.

Security technology	**Aware respondents**
Data Encryption Standard (DES)	80%
Digital / electronic signature	64%
Certification Authority (CA)	50%
Secure Electronic Transaction (SET)	42%
Trusted Third Party (TTP)	33%

Table III: Awareness of security technologies

Respondents were also asked for their opinions on the importance of different security safeguards for e-commerce. Only 55% of respondents attempted this question, the responses to which are summarised in table IV (note that the figures indicate the number of respondents rather than percentages).

	Importance				
	1 (high)	**2**	**3**	**4**	**5 (low)**
Secure communication	13	10	8	2	2
Authentication of you by vendor	2	5	5	9	12
Authentication of vendor by you	8	4	11	7	5
Against fraudulent	7	7	6	8	5
Non-repudiation	4	9	3	8	10

Table IV: Consumers ranking of security features

The issue of secure communications is clearly the biggest concern and it is interesting to compare this finding with the corresponding response from businesses that is presented in the next section. The significant proportion of respondents who indicated that authentication of them by the vendor was not an important concern implies that they would not object to someone else masquerading as them in a transaction. In addition, the largely negative view regarding the requirement for non-repudiation is also surprising. It is the authors' opinion that some respondents did not fully consider or understand these issues.

Having previously established that the majority of respondents possessed credit cards, a later question attempted to assess their opinion of using it in different contexts. The scenarios considered were face to face transactions, via a third party (e.g. via a waiter in a restaurant), over the telephone and via the Internet. The respondents were requested to rate the perceived user-friendliness and security of each using good, medium or poor rankings. Table V presents the results of this exercise.

User-friendliness				
	Face to face	**Via third party**	**Over telephone**	**Via Internet**
Good	53	32	19	21
Medium	4	26	34	24
Poor	3	3	8	16
Security				
	Face to face	**Via third party**	**Over telephone**	**Via Internet**
Good	36	9	8	9
Medium	22	34	26	25
Poor	2	18	25	27

Table V: Perceived user-friendliness and security of credit card transactions

It can be seen that in overall terms, the Internet fares worst in terms of both user-friendliness and security. The latter observation is particularly revealing, because in terms of the actual protection afforded to the card details, the Internet is probably a safer option than the third party and telephone options. With these results in mind, a follow-up question posed the same user-friendliness / security issue in respect of other Internet / electronic payment technologies (namely smart cards, electronic cash (e.g. DigiCash) and SET). Table VI shows the responses obtained, again indicating the number of respondents rather than percentages (note that some respondents did not answer all questions here, even though a 'Don't Know' option was available in each case).

	User-friendliness			
	Good	**Medium**	**Poor**	**Don't know**
smart card	30	17	4	13
e-cash	18	28	1	13
SET	16	12	5	27
	Security			
	Good	**Medium**	**Poor**	**Don't know**
smart card	27	15	5	15
e-cash	8	28	8	16
SET	20	12	2	27

Table VI: Perceived user-friendliness and security of electronic payment technologies

The 'Don't know' option was included in this case to take account of the fact that respondents might not be aware of certain technologies. This proved to be particularly the case with SET technology, which suggests a possible reason why credit card transactions via the Internet were deemed to be an insecure proposition in table V.

Finally, respondents were asked to indicate their expectations regarding the measures that Internet commerce sites should take in relation to customer privacy. As expected, this produced a strong response, with 87.5% indicating that they would expect comprehensive information regarding the site's security and privacy policy. Use of personal information was also a key consideration, with 81% wanting a chance to choose whether it could be used for purposes other than the conduct of the transaction (e.g. addition to mailing lists).

Published in Internet Research, *Internet Research*, vol. 9, no. 5: 372-382 1999

A SURVEY OF BUSINESS

Background and procedure

A second survey was also attempted, this time targeting UK businesses, with the intention of assessing commercial attitudes. Good scene-setting information for this exercise is provided by the results of the 1998 KPMG Information Security Survey, in which respondents were asked to assess a range of business issues in terms of their importance and likely impact upon the organisations. Electronic commerce was considered to be the most important issue (cited by 23% of organisations), ahead of other areas such as mobile computing and the Year 2000 issue (KPMG, 1998). However, the same survey discovered that many organisations using the Internet are not aware of the associated risks.

The focus of the questions posed in the second survey presented here was somewhat different from the survey of consumers, the reasons being:

- an attempt had been made in the consumer questionnaire to minimise the occurrence of technical questions as the majority of likely respondents were assumed to be non-specialists. However, the target audience for the business survey was technical decision-makers and, as such, this constraint was removed.

- some questions, such as those about an organisation's policy in managing its IT network, were only suitable for business professionals.

In this case, a total of 26 questions were involved, with the objectives of assessing:

- the respondent (organisation's) background and expertise in the field;
- the organisation's policy of doing online business and their reasons;
- the organisation's concerns in online business;
- the respondent's policy for security in their internal network, and whether they are aware of any standards in information system security;
- the respondent's view on e-commerce security: the security and payment technology that are currently available, and what they think is important to be provided;
- the respondent's opinion on the current issue of key escrow.

A total of 120 paper-based questionnaires were distributed, targeting organisations throughout the UK. In addition, an online version was again made available. However, the results were somewhat disappointing, as only nine organisations responded to the postal survey and no responses were received on the WWW site (representing a total response rate of only 7.5%). The authors consider that the most likely reason for this was that many businesses were not willing to respond for fear of revealing their organisational security strategy. In addition, it is felt that many UK businesses may currently be waiting for the 'right time' to engage into e-commerce and may consequently not have an opinion on the questions being asked of them.

Results

In view of the very small number of responses, it was not possible to conduct an analysis of the same nature as had been undertaken for the end-user results. As such, a series of more general observations were drawn from the results and are presented below. It is suggested that these should be interpreted as indicative rather than definitive opinions from the business community.

All respondents were at a middle or senior level within their organisation and possessed a generally high level of education (graduate level or above). Most claimed that having Internet access in their organisation is a valuable tool for the business and gives competitive advantage. As expected, the most popular use of the Internet within the companies was for general information search and retrieval activities. A number of questions were also posed in relation to the organisation's views about use of the Internet for online purchasing and advertising/sales activities. The results suggested that most companies purchase online because it is more convenient. Other views expressed were the attractiveness of online offers and the access to a wider range of suppliers. In terms of advertising or sales activities, the primary reasons cited (by almost all respondents) were access to a global market, possibilities for attractive presentation and cost. Approximately half of the respondents claimed to engage in business-to-business e-commerce activities. A similar proportion indicated that they supported direct sales to customers via their web sites. However, when asked to rate the security requirements of these activities on a low-medium-high scale, more than two thirds of the companies rated the requirement as 'low' (while the remainder said 'medium'). This lack of concern is both surprising and worrying and it is considered that such views would be unlikely to give confidence to customers.

The questions then moved on to consider security issues and concerns relating to e-commerce. Almost all respondents were concerned about internal system vulnerability, external communication security, and customer authentication. Approximately half of the respondents expressed concern about negative publicity from media/press and the lack of predictable legal environment governing electronic commerce. One respondent cited the speed of the WWW as a potential concern.

In terms of network security, all respondents were concerned about attacks from outsiders, while two thirds were also wary of insider attacks. The latter opinion is warranted in view of frequently cited evidence to suggest that the majority of computer abuse incidents are perpetrated by an organisation's own staff (Audit Commission, 1998). Viruses and system unavailability were of minor concern (presumably on the basis of appropriate safeguards already being in place). All respondents claimed to use user authentication, access control and security policy measures to lessen the IT network risk, and all bar one also employed a firewall. Other measures cited included virus controls and auditing.

For organisations offering e-commerce services, the preferred security technology was Secure Sockets Layer (SSL), used by two thirds of respondents. The more robust and purpose-designed SET approach was used by a third of respondents (with some respondents indicating that they incorporated both).

The businesses were also posed the same question as the end-users in terms of ranking the importance of different security measures (see table VII). Only a subset of the respondents attempted this question and, therefore, the results are even less reliable if extrapolated to a wider population. However, it is interesting to note that, within this sample, some of the perceptions are in marked contrast to the results from the user survey. For example, the issue of secure communications, highlighted as by far the most important consideration for consumers, is ranked relatively low by all bar one of the respondents here.

	Importance				
	1 (high)	**2**	**3**	**4**	**5 (low)**
Secure communication	1	0	2	2	1
Authentication of customer	1	2	2	0	1
Authentication of vendor	1	3	0	2	0
Against fraudulent	1	2	0	1	2
Non-repudiation	2	0	1	2	0

Table VII: Business ranking of security features

The survey was conducted at a time when the UK Government was proposing e-commerce legislation that included the recommendation to adopt key escrow technologies. As such, some questions were posed in relation to this issue and the licensing of Trusted Third Party (TTP) services. Two respondents agreed with UK government's stance at the time (i.e. that the use of licensed TTPs would require the escrowing of encryption/digital signing keys and that only individuals/organisations using licensed services would be able to rely on legal status of their digital signatures). By contrast, three respondents agreed with the European Commission's draft on the issue (European Commission, 1997), which recommends separation of the issue of digital signature from that of data encryption in terms of legal restrictions. The remaining respondents were unable to offer an opinion on the TTP issue. However, most respondents were in agreement that key escrow harms a client's privacy. It should be noted that, at the time of writing, it was not clear whether or not key escrow would remain a feature of the UK legislation (Bicknell, 1999a).

Most respondents felt that commerce sites should contain comprehensive information for consumers regarding security and privacy policy, and approximately two thirds felt that consumers should have the opportunity to express a preference as to whether their personal

details could be put to additional uses. These views can be seen to be generally in line with the feelings expressed by consumers in the first survey.

DISCUSSION

Given the more significant response rate involved, the main basis for further analysis comes from the consumer-focused survey. It is interesting to assess more closely how respondents' security concerns and their awareness of security technologies affected their attitude to shopping online. This is illustrated in figures 1 and 2 below. Figure 1 depicts the security concerns expressed by credit/debit card holders and indicates the proportion in each case that were online shoppers.

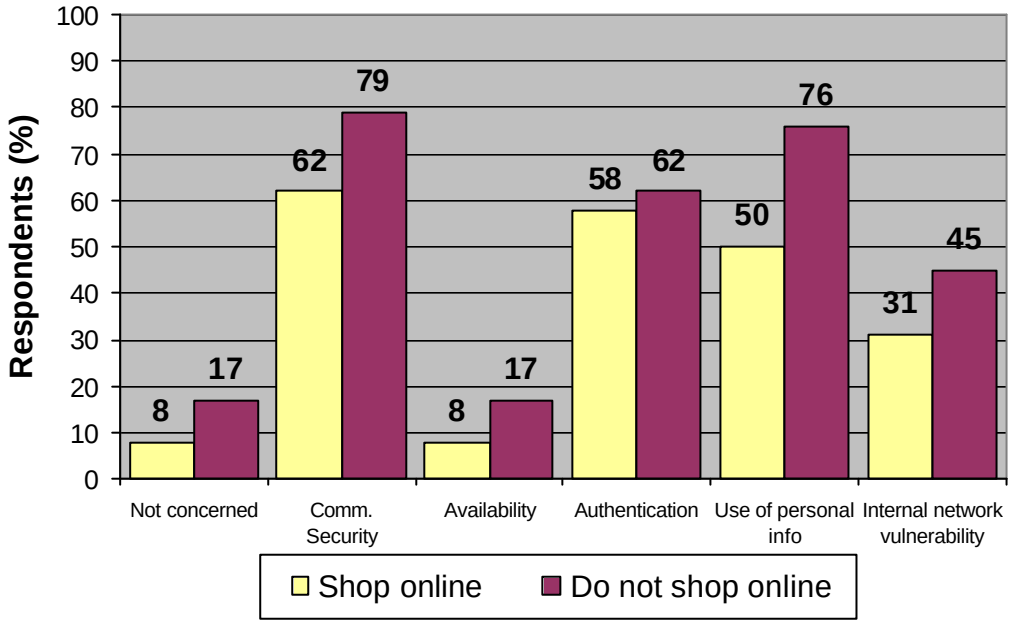

Figure 1: Online shopping in relation to security concerns

Of the 47% of credit card holding respondents who are online shoppers, 92% of them have some form of security concern. The fact that this concern has not prevented them from engaging in the activity suggests that, from the customer perspective, the benefits of online shopping clearly outweigh the risks.

As the figure shows, respondents who do not shop online exhibited a greater level of concern and it can be conjectured that actually participating in online commerce would remove some of their doubts. However, it is also important to avoid making the assumption that their security concerns are the only reasons these respondents do not shop online. Various other factors, such as the lack of an Internet connection at home or simply not having encountered the need to do so, could be equally valid explanations. This is illustrated to an extent by the fact that, even

amongst the small number of respondents with no concern about security, the majority are still not online shoppers. Upon reflection, the authors regret not having included a specific question such as "Has concern about security prevented you from shopping online?" within the survey, which would have enabled a more definitive view to be formed.

Figure 2 considers all respondents and examines awareness of security technologies, again indicating the proportion of online shoppers.

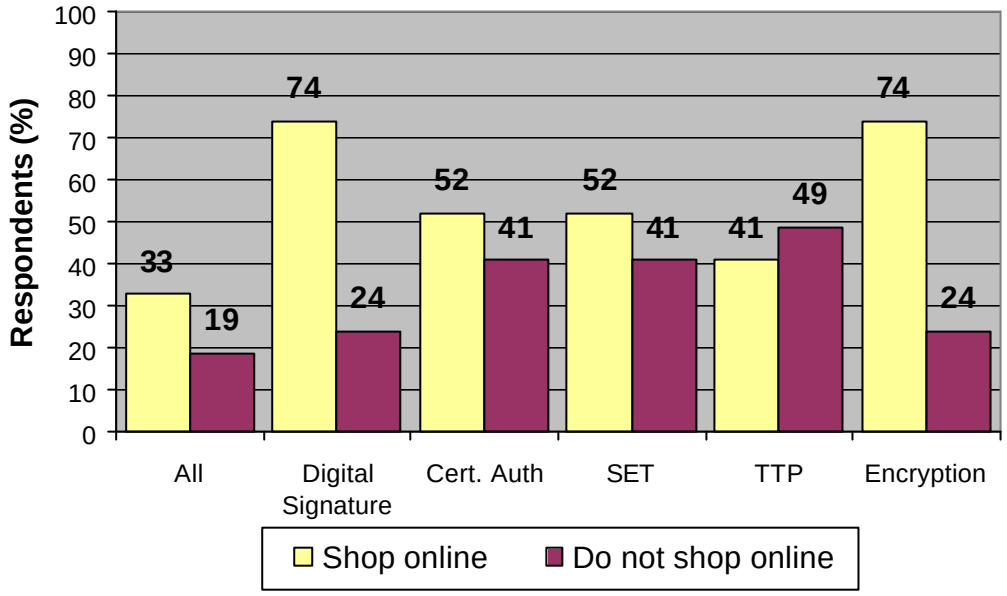

Figure 2: Online shopping in relation to security awareness

These results almost exclusively suggest that consumers with a greater awareness of security technologies will be more likely to shop online. The only exception in the results observed was in relation to Trusted Third Party services, where those who had heard of the concept were less likely to shop online. There was no clear reason for this, but a possible explanation relates to the fact that respondents may have been influenced by the rather negative coverage of TTPs in the UK computing press and general media, where the issue is closely linked with the controversial topic of key escrow.

A major conclusion that can be drawn from the results is that awareness is key to increasing consumer confidence. The survey results suggest that if more were known about the security features employed on the Internet then it would encourage significantly more people to buy online. In addition, it would help to allay the fears of those who are purchasing online despite security concerns about doing so. It is also considered that improved awareness would encourage further participation of businesses. However, work is required to improve upon the current situation. For example, even with the more security-aware 'online shopper'

respondents from figure 2, there were only two cases in which significantly more than half of the respondents had heard of the security technologies under consideration. This is curious, as one would expect them to be more informed and the lack of awareness exhibited is analogous to traditional credit or debit card customers being unaware of security safeguards such as signatures and PIN numbers. The initiative to improve the situation should be taken by online vendors themselves (in order to improve the confidence of their potential customers) and by parties such as credit card companies, whose assurance would serve to encourage both consumers and businesses. The latter can already be seen to be active in terms of the development of the SET standard and its promotion on their WWW sites (see, for example, www.visa.com). However, wider, mass media promotion is probably appropriate at this stage, because many parties with security concerns will not see the information if they have to go to the credit card companies WWW site to do so.

It was conjectured earlier in the paper that UK businesses may be waiting for the 'right time' to engage into e-commerce. Possible reasons for this include:

- a belief that consumer lack an understanding of e-commerce, especially on the issue of security and privacy (Anderson Consulting, 1998);
- a lack of understanding and support from government on the legal and liability issues.

However, it should also be remembered that (a lack of) security does not represent the barrier to successful and credible e-commerce. Consumer trust can also be affected by a lack of confidence in the general credibility of online vendors. Even with appropriate security technologies, many online services may still be perceived as lacking a 'track record' in their market. Even where reputable online brand names have been established (or where traditional brands have established an online presence), the Internet environment offers opportunities for these efforts to be undermined in ways that would not be possible in the traditional marketplace. For example, sites such as the pioneering online bookseller, Amazon.com, have witnessed the establishment of copycat sites, registered by competitors using country-level domains outside the United States (e.g. www.amazon.gr, a site established in Greece, selling similar products to the original Amazon, but having no connection to the recognised company). This may be confusing for potential consumers, as well as harmful for the business that has been 'copied', whose reputation may suffer as a result (Bicknell, 1999b).

CONCLUSIONS

Electronic commerce is a domain with significant promise for future development. As more people gain access to the Internet, the base of potential online customers can only increase. However, the issue of security will remain a concern in the short term, as most people do not have a substantial knowledge of what is really happening in this online world. What they hear from the media often refers to security breaches and frauds and, as a consequence, an environment of trust has yet to be established. This is not necessarily because of a lack of

confidence in the security technologies themselves, but because, in many cases, people are not sufficiently aware of the possible protection that exists. This is supported by the results of the survey conducted, which shows that even current online shoppers are concerned about security problems. In addition, there are more people who do not shop online at all because of security worries.

Businesses are very much aware of the advantages that the Internet can deliver in a commerce environment, but are also aware of the security issues. While safeguards have been incorporated to protect online transactions, the limited results obtained in this investigation suggested that the security concerns of businesses were not necessarily in line with those of their potential customers. As such, some harmonisation is required to increase confidence. Another important factor for companies is a conducive environment (such as support from government) to support them in conducting online business.

The years ahead will witness the resolution of these issues, as the norms of the electronic commerce market are established and more widely understood by the parties involved. While security will undoubtedly be one of the more complex barriers to be overcome (particularly at an international level), the authors are confident that the momentum of the Internet and the web in general will ultimately force a solution. At this point, the electronic environment will form the primary basis for commerce of the future.

REFERENCES

Anderson Consulting. (1998), "Your Choice. How eCommerce Could Impact Europe's Future". Anderson Consulting. http://www.ac.com/services/ecommerce/ecomrept.pdf

Audit Commission. (1998), "Ghost in the Machine – An Analysis of IT Fraud and Abuse". Audit Commission Publications, UK. February 1998. ISBN 1-86240-056-3.

Bicknell, D. (1998), "Security flaw strikes at E-commerce users", *Computer Weekly*, 2 July 1998, p2.

Bicknell, D. (1999a), "MPs to release report early in bid to kill off key escrow", *Computer Weekly*, 13 May 1999, p2.

Bicknell, C. (1999b), "E-commerce Pirates on the Prowl", *Wired News*, 12 May 1999. http://www.wired.com/news/news/business/story/19600.html.

Chelmsford, J. (1999), "Forward", *Electronic Commerce & Public Policy*. Supplement to Information Technology & Public Policy, Journal of the Parliamentary Information Technology Committee. Spring 1999, p1.

Dierks, T. and Allen, C. (1999), "The TLS Protocol Version 1.0". RFC 2246, The Internet Society, January 1999.

DTI. (1999), "Building Confidence in Electronic Commerce – A Consultation Document". Department of Trade & Industry. Document reference URN 99/642.

European Commission. (1997), "Ensuring Security and Trust in Electronic Communication – Towards a European Framework for Digital Signatures and Encryption", European Commission Directorate-General XIII, COM (97) 503.

Frier, A.; Karlton, P.; and Kocher, P. (1996), "The SSL 3.0 Protocol", Netscape Communications Corp., Nov 18, 1996.

Hancock, B. (1999), "Security Views", *Computers & Security*, Vol. 18, No. 3, pp184-198.

Howell, D. (1998), "Cash in your chips", *T3*, August 1998, pp51-53.

KPMG. (1998), "Information Security Survey 1998", KPMG Information Risk Management, London, UK. http://www.kpmg.co.uk.

Ratnasingham, P. (1998), "The Importance of Trust in Electronic Commerce", *Internet Research*, Vol. 8, No. 4, pp313-321.

SETCo. (1997), "SET Secure Electronic Transaction Specification - Book 1: Business Description", Version 1.0. 31 May 1997. http://www.setco.org/set_specifications.html