Actual and perceived levels of risk in consumer e-commerce

Pita Jarupunphol and Chris Mitchell

Information Security Group
Royal Holloway, University of London, UK
E-mail: P.Jarupunphol@rhul.ac.uk; C.Mitchell@rhul.ac.uk

ABSTRACT

Most consumers perceive e-commerce as the riskiest shopping method in comparison with other methods of payment. Confidentiality of credit card numbers is an overriding issue restricting consumer participation in e-commerce. As a consequence, it is imperative to measure the levels of risk in e-commerce and other shopping methods. This study is an analysis of perceived and genuine risks associated with e-commerce. The levels of risks perceived by consumers in various shopping methods including Internet shopping are described, as are the levels of actual risk. The differences between the two are considered, and methods of dealing with the differences are given.

Keywords: Electronic Commerce (E-Commerce), security, encryption, cryptographic algorithms, actual risk, perceived risk, risk perception gap, Secure Sockets Layer (SSL), Secure Electronic Transaction (SET).

INTRODUCTION

E-commerce is an innovative business model that is driving organizations to transform their core business functions to remain profitable. In addition, it provides many useful functions, which facilitate a number of business activities, according to Ghosh (1998). Increasingly many companies are utilizing e-commerce technology as a medium of conducting business since it has advantages for both the supplier and the consumer. The emergence of e-commerce technology makes it easier for consumers to engage in online shopping because of the lower cost and ease of acquisition of products or services via the Internet

Although e-commerce provides many benefits to consumers, e.g. convenience, greater choice, lower prices, and more information, there are also a number of barriers restricting its growth. The fact that breaches of Internet security are reported with great frequency means that there is a danger that potential users will be reluctant to engage in e-commerce because of fears about security. This means that user trust is a key enabler for the growth of the e-commerce market. Nonetheless, the real level of risks in e-commerce world and the level of risks perceived by consumers are still uncertain. Ideally, the risks involved in an e-commerce transaction should be no greater than the risks in a conventional transaction. The main objectives of this paper are as follows:

- to assess the main risks for home users engaging in Internet e-commerce;
- to assess home users' perceived levels of risk for various types of commerce, including e-commerce;
- to understand whether a disparity between the real and perceived risks exists.

For the purposes of this paper we assume that e-commerce payments are made using credit or debit cards. Whilst other forms of payment exist, debit/credit will probably remain the dominant payment method for some time to come.

POTENTIAL E-COMMERCE PARTICIPANTS

Recently, e-commerce has become a strategic tool for companies wishing to generate trade from the electronic consumer (e-consumer) on the Internet. The main requirement for a home user to engage in e-commerce is that the user has a connection to the Internet. We therefore suppose that all users with

Internet access are potential e-commerce participants. Based on this assumption, Figure 1 shows that there are more than four hundred million potential e-commerce participants.

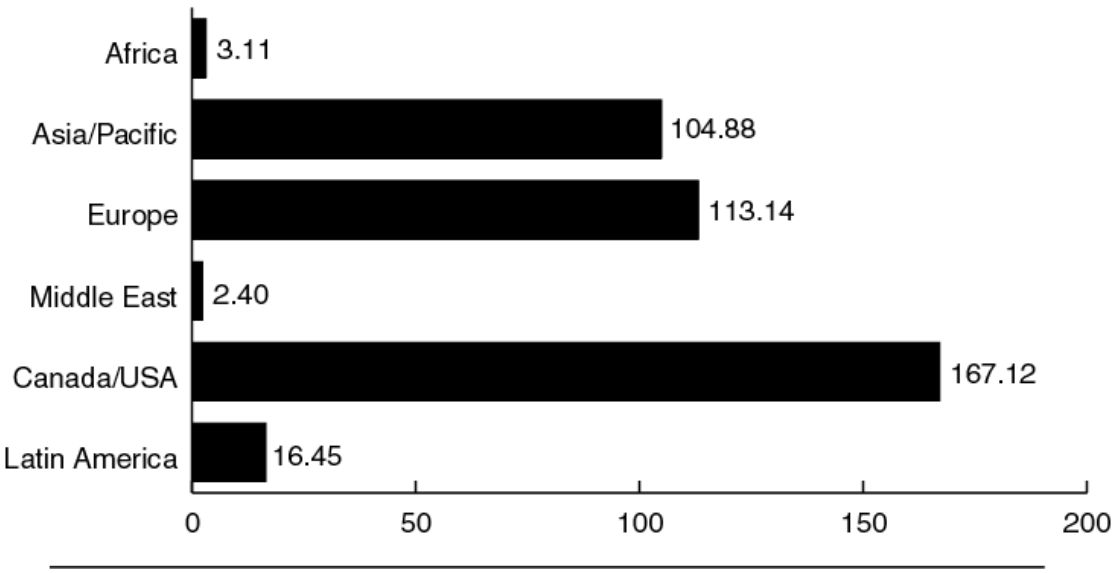

Figure 1: Global Internet Population (millions).
Source: Surveys, November 2000 (http://www.nua.ie)

Although there are various methods of accessing the Internet, we assume here that the home user connects to the Internet using a Windows-based PC equipped with a modem, and that web accesses are performed using a popular browser such as Internet Explorer or Netscape Communicator. Whilst a variety of access devices can be used, 56k modems are currently the most popular means of access (see Figure 2).

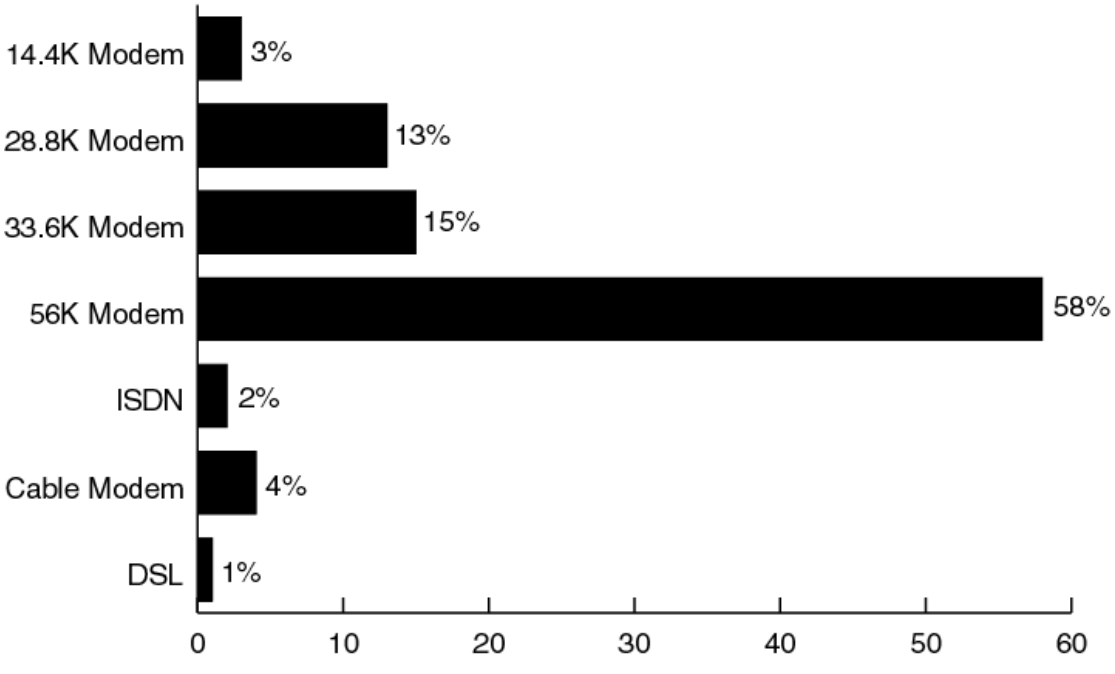

Figure 2: Devices used to connect to the Internet.
Source: About.Com, August 1999 (http://internet.about.com)

PERCEIVED RISKS IN E-COMMERCE

Human perceptions of e-commerce risks vary widely, just like other human characteristics. Some people believe that e-commerce is worth participating in because it offers several useful functions, such as convenience. On the other hand, others perceive e-commerce as being too risky. A survey of 2,810 adults was conducted by Harris Interactive Survey (http://www.harrisinteractive.com) in August 2000 to examine consumer perspectives regarding e-commerce. For example, they asked how many times that potential e-commerce participants had ordered online in the last twelve months, and where relevant the reason why they had never purchased via e-commerce. In addition, the survey also covers the types of information that need to be protected in e-commerce from the consumer perspective. The results are summarised in Figure 3.

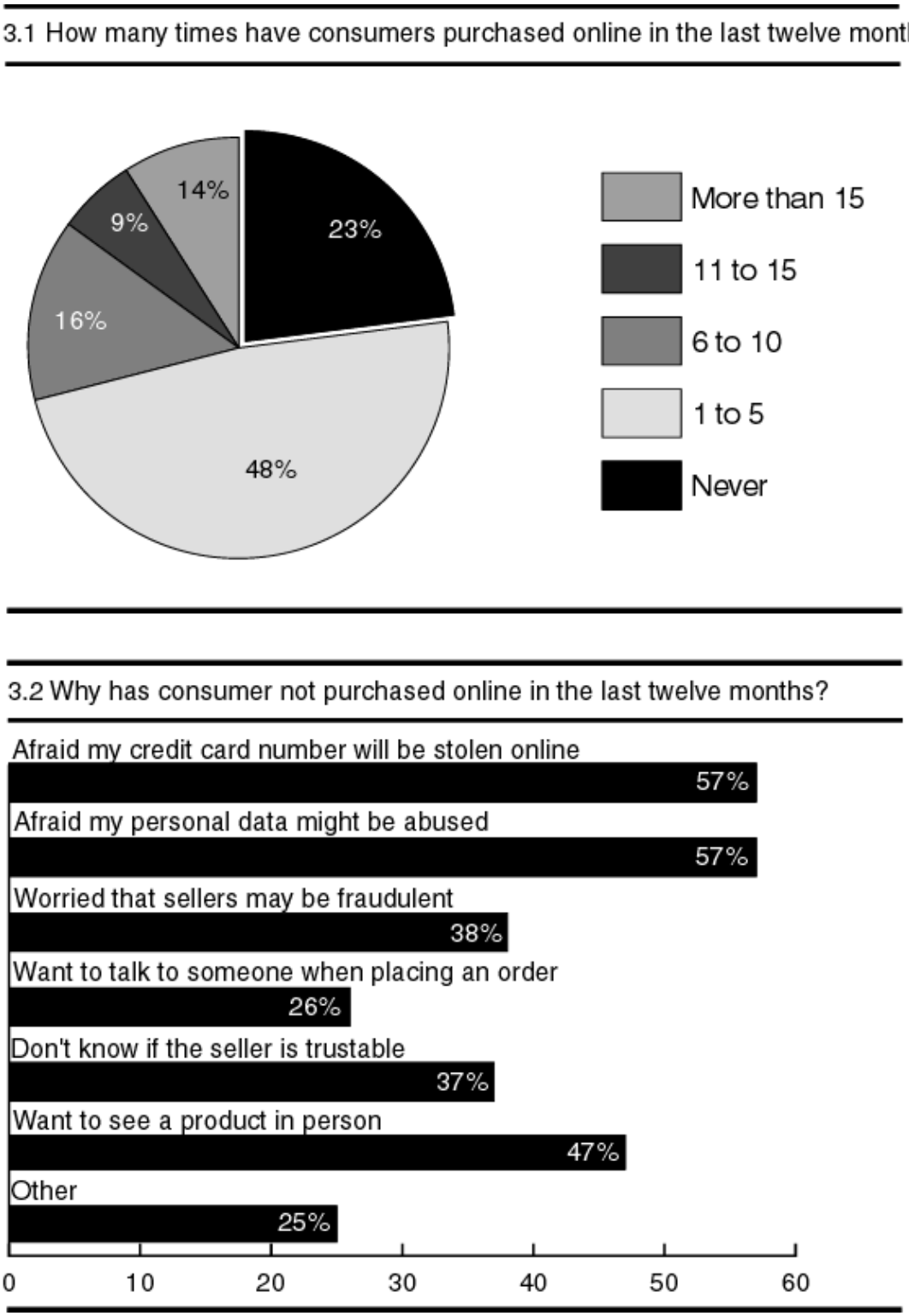

Figure 3: Consumer attitudes to Internet shopping.
Source: Harris Interactive, August 2000.
Participants: 2,810 Internet users, more than 18 years old

E-commerce and other methods of payment

As shown in Figure 3, there are many reasons restricting consumer participation in Internet shopping, such as sensitive information breach, merchant fraud, and social requirements. It can be seen that twenty-three percent of participants have never placed an order online in the last

twelve months. Furthermore, forty-eight percent have ordered less than six times in one year. In such cases, trust in e-commerce is likely to be relatively low.

While the overall level of consumer confidence in e-commerce is still unclear, a survey conducted by the National Consumer Council Survey (http://www.ncc.org.uk) in April 2000, summarised in Figure 4, illustrates that most people believe that e-commerce is the riskiest shopping method in comparison with other traditional shopping methods, such as shopping over the telephone and using catalogues. Shopping centres are considered the safest shopping method.

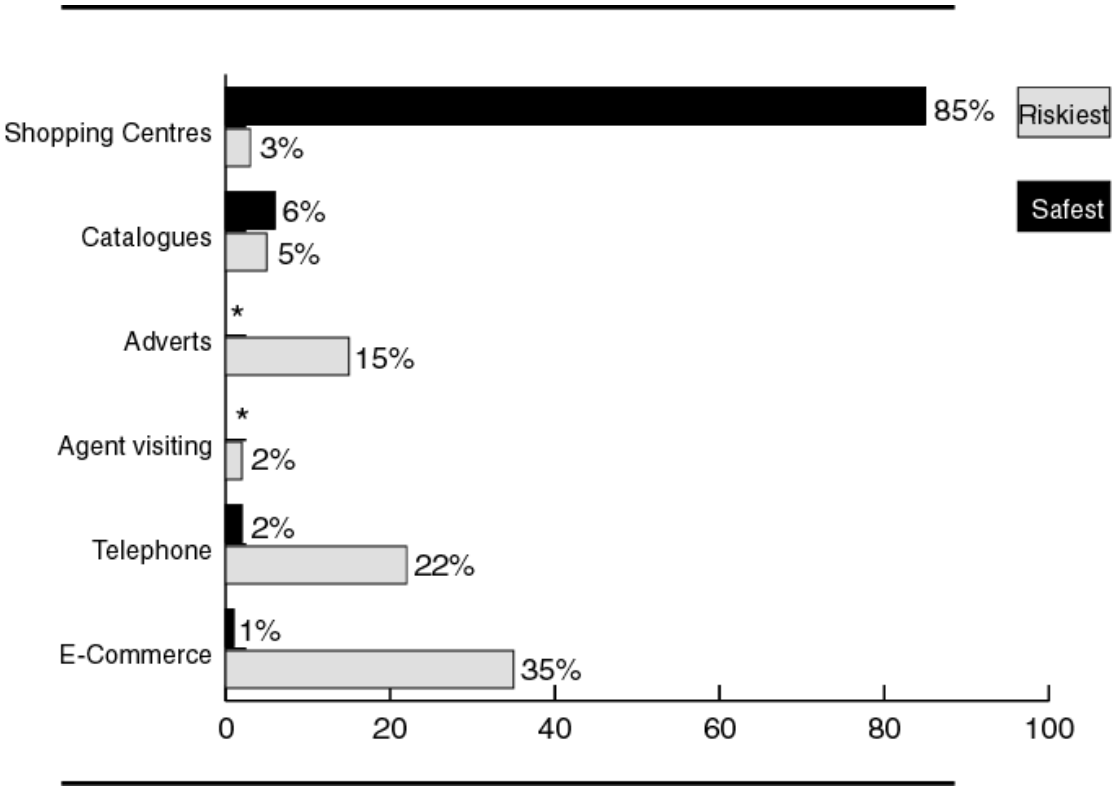

Figure 4: Consumer attitudes to Internet shopping and other shopping methods. Source: NCC/MORI, April 2000.
Participants: all (1,950), Internet users (513)

In summary, the perceived risks associated with Internet shopping are greater than that for other shopping methods. Theft of credit card numbers is the overriding concern. Consequently, it is interesting to find out which process in online shopping consumers perceive as the most vulnerable. A survey conducted by Harris Interactive, summarised in Figure 5, also shows that the interception of sensitive information during transmission from consumer's computer to merchant's server is most commonly considered as the weakest link in e-commerce.

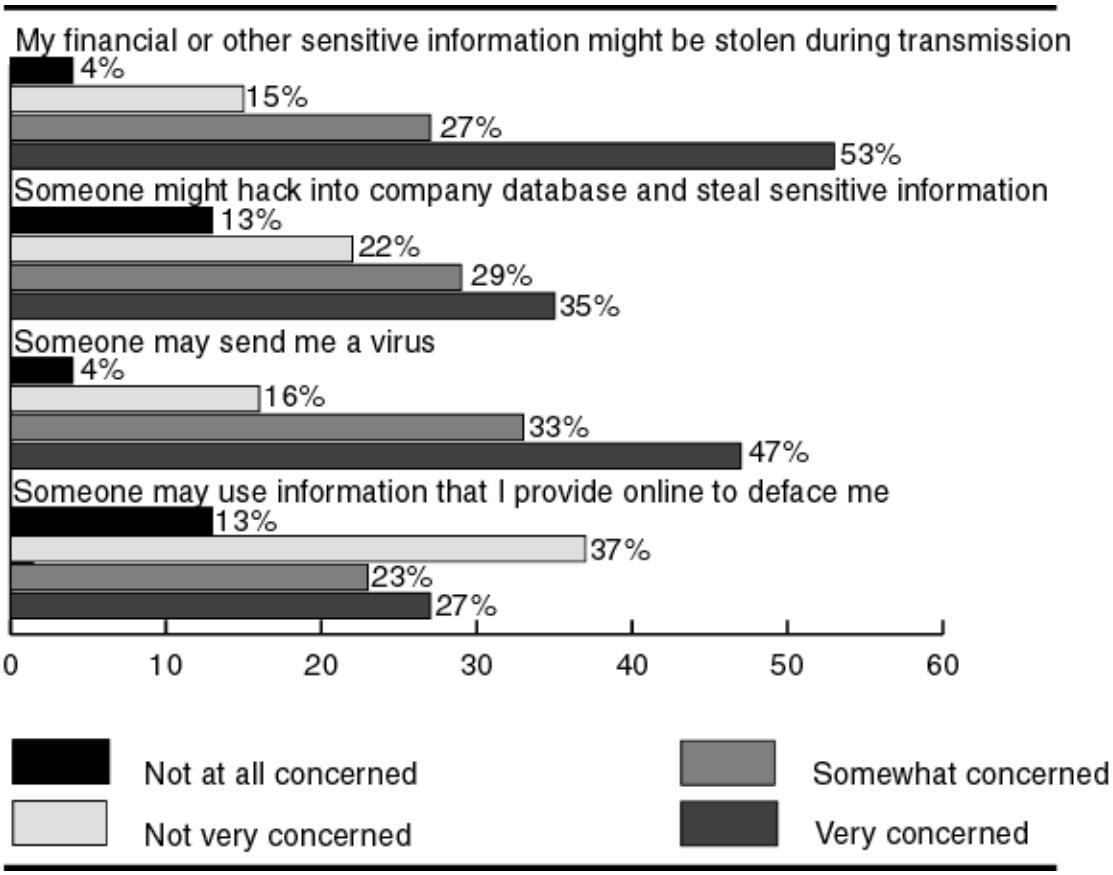

Figure 5: Consumer concerns regarding Internet security.
Source: Harris Interactive, August 2000
Participants: 2,810 Internet users, more than 18 years old

From the information in the above figure, it would seem that most consumers are particularly concerned about the security of data transmission in e-commerce. This is consistent with Tomlinson (2000), who states that numerous consumers believe that security breaches occur during transmissions between clients and servers. This is despite the fact that e-commerce security encompasses a number of other aspects, including client-side security, merchant server security, application security and transaction security, (Ghosh 1998).

Sensitive information of concern to Internet users

In spite of the fact that e-commerce systems allow consumers to place an order directly through Internet systems, many potential users of e-commerce are hesitant to provide e-commerce merchants with their sensitive information. Friedman et al. (2000) state that lack of financial and security confidence are reducing consumer acceptance of this innovative online shopping technology. Figure 6 demonstrates what types of sensitive information are most in need of protection. Clearly, the confidentiality of credit card numbers, social security numbers, and personal financial information are of greatest importance to users.

Other issues

Whilst loss of personal data confidentiality during transmission is an overriding concern for consumers, there is another associated factor causing negative consumer perceptions of e-commerce. This is the inflammatory reporting of computer security incidents in the popular press. For example, instances of credit card fraud involving Internet use are often given very wide press coverage, out of proportion to their importance (Ghosh 1998).

Many information security experts argue that compromise of sensitive information in e-commerce is not likely during transmission, but through insufficient protection of merchants' web servers. According to (Caldwell 2000) in CommerceNet (http://www.commercenet.com/research), the theft of credit card numbers during transmission over the Internet is popularly perceived as the main concern to credit card fraud. In fact, credit card fraud often occurs at merchant web servers. This is the first example of where consumer perceptions of risk and the actual level of risk are rather different.

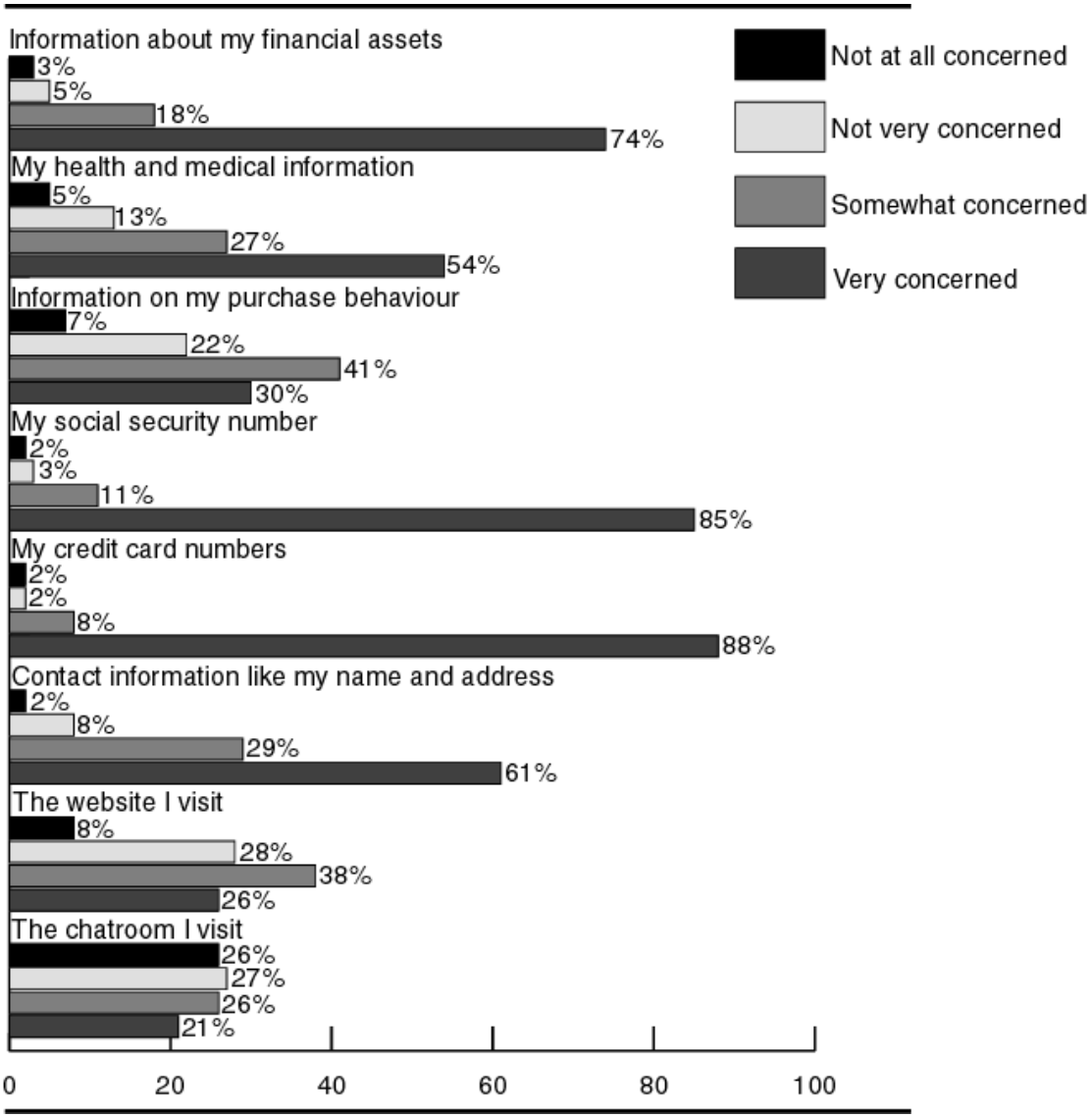

Figure 6: Consumer concerns regarding protection of information.
Source: Harris Interactive, August 2000.
Participants: 2,810 Internet users, more than 18 years old

ACTUAL RISKS – CREDIT CARD FRAUD IN E-COMMERCE

We next consider the actual levels of risk associated with credit card transactions of both e-commerce and the more conventional types.

Transaction fraud risks

We start this analysis of actual risks by considering the levels of fraud in credit card transactions. From eMarketer (http://www.emarketer.com) of November 2000 we learn that Visa and MasterCard report rates of credit card fraudulent transactions of 0.08% and 0.09% respectively, for all types of

transaction. As far as e-commerce credit card transactions are concerned, eMarketer from January 2001 reports that of 60,320,000 online B2C transactions in 1999, only 18,600 (i.e. 0.03%) were fraudulent.

It would thus appear that the risk of fraud per transaction is actually significantly lower for online transactions than for other types of transaction. Thus one might conclude that, at least with respect to the proportion of fraudulent transactions, e-commerce is actually one of the less risky forms of commerce. In the next section we examine specific types of conventional transaction in more detail, to discover which are actually the most risky.

Actual risks - technology assessment

It has been shown in the previous section that the incident rate of credit card fraud is low in comparison with conventional transactions. That is, the actual relative risks would appear to be directly opposite to consumer perceptions of relative risks. We now consider various types of transaction in a little more detail so as to understand better the real risks involved. We focus here, as throughout, on credit and debit card transactions.

In a high street transaction the retailer has access to a user's credit card for a short period of time, and therefore has the opportunity to copy all the information on the card. Moreover, the retailer will also have a copy of the transaction details, as needed for clearing and settlement, which again will contain most of the information on the card. Similarly, in a telephone transaction the retailer has access to a user's credit card number because this information must be passed to the retailer over the telephone in order to complete the transaction.

Credit card information transmitted over the Internet, however, seems to have more layers of protection in comparison with using credit cards to make payments in shops or when sending credit card numbers via telephone to place an order. According to Stein (1998), there are two main security protocols used to provide transaction security, namely Secure Sockets Layer (SSL), established by Netscape, and Secure Electronic Transaction (SET) created by Visa and MasterCard. Although both these protocols protect e-commerce transactions against potential eavesdroppers, SSL and SET work very differently. Also, while SSL is widely used, SET has not really been adopted.

During data transmission using the SSL protocol, cryptographic algorithms applicable to SSL, such as the Data Encryption Standard (DES), triple DES, and IDEA, are used to encrypt all data sent between the relevant parties (Hassler 2000). By this means, consumers are assured that their credit card numbers and other related sensitive information will be unreadable to an interceptor. SSL has different encryption key lengths varying from 48-bit to 128-bit, and its performance in securing data transmission is dependent of the lengths of the key. According to Burnett et al. (2001), 128-bit SSL encryption appears sufficiently secure to resist all attempts to break it, at least with current cryptanalytic techniques.

COMPARING ACTUAL WITH PERCEIVED RISKS

Perceived risks

E-commerce is perceived as the riskiest shopping method. Most consumers believe that the chance of credit card fraud in Internet shopping is high. Perceived risks in e-commerce can be summarised as follows:

- e-commerce is very risky by comparison with other methods of payment;
- loss of confidentiality of credit card information is the main issue.

Actual risks

By contrast, it has been shown that the credit card fraud rate in online transactions is actually low by comparison with the rate for conventional transactions. As a result, actual risks in e-commerce can be briefly summarised as follows:

- credit card fraud in e-commerce cannot happen as easily as consumers fear;
- the level of actual risk in e-commerce is indeed lower than the levels of risk perceived by e-commerce consumers.

DEALING WITH THE RISK PERCEPTION GAP

As discussed above, the levels of perceived risk associated with e-commerce are very different from the levels of genuine risk. Most consumers are concerned that their credit card numbers can be compromised during transmission on the Internet. Furthermore, there is also other sensitive information, such as social security numbers and information about financial assets, for which sufficient protection is required to ensure consumer confidentiality, acknowledged as the key security goal for e-commerce merchants. As stated by Bhatnagar et al. (2000), an organisation wishing to succeed in this new business era needs to have a clear understanding of how to build up consumer confidence. In order to increase consumers confidence, it is important to consider how to deal with the difference in levels between actual risk and perceived risk (the 'risk perception gap') in e-commerce. This is the focus of the remainder of the paper.

Statement of consumer confidentiality

According to the Data Protection Act of 1998 as cited in Schneier (2000), 'organisations are prohibited from the collection, use, and dissemination of personal information without the consent of the person, and also have the duty to tell individuals about the reason for the information collection'. Similarly, consumers need to be assured that their sensitive information will remain private. A statement of consumer privacy must be placed in the e-commerce website in an obvious location. Consumers need to be assured that their information will not be exposed or used for any other purposes without their authorisation.

Techniques and tools for secure e-commerce

E-commerce merchants must employ appropriate methods to deal with the threats jeopardising e-commerce systems. It is the responsibility of e-commerce merchants to support the latest security techniques and tools to ensure consumer confidence. For example, e-commerce merchants should use SSL with 128-bit rather than shorter keys, to assure consumers that their private information will be secure against eavesdropping by even the most determined attackers. Merchants should consider making prominent statements about the techniques and tools they employ to ensure security.

Reporting problems with e-commerce

Broadcasters responsible for issuing material related to security weaknesses in e-commerce have a duty to be sufficiently well-informed to ensure that their reports are reliable and consistent with the real problems. For example, most credit card fraud cases in e-commerce occur because of weaknesses in merchant servers rather than interception of data transmission, which is securely protected by SSL or Secure Hypertext Transfer Protocol (S-HTTP) (Oppliger 2000). Broadcasters therefore need to understand the reasons for any security breaches in e-commerce, so that they can alert users to the real threats.

Solving the actual problem

It cannot be assumed that consumers, who are so concerned with security in data transmission, will be comfortable with the fact that breaches of sensitive information occur at the merchant server. Information stored in merchant servers must be appropriately protected to ensure that customer confidence is not damaged by actual attacks. As a result, dealing with the risk perception gap requires the real risks to be addressed, as well as those perceived as most serious by consumers.

Government support

There are numerous e-commerce merchants, and there are also many different tools and techniques employed by merchants to secure their online e-commerce infrastructure. These different techniques will have varying degrees of effectiveness in dealing with security threats, and consumers will have the problem that they have no idea how secure each merchant is. It would therefore increase consumer confidence if government regulation (and/or codes of practice) could be used to enforce minimum levels of security protection for e-commerce sites. One might envisage the development of a 'special version' of security baseline standards such as BS 7799-1 (=ISO/IEC 17799), applying particularly to e-commerce merchants. Merchants could then display prominent notices on their web sites, claiming adherence to the relevance baseline documents.

SUMMARY AND CONCLUSIONS

It is clear that the level of e-commerce participation is critically dependent upon consumer confidence in e-commerce security. Many consumers fear that their financial information will be compromised due to lack of security in online shopping. Levels of perceived risk, which may increase or decrease, are determined by the levels of confidence that consumers have in this innovative business. An e-commerce organisation should focus on strategies that can build up consumer confidence, so that security and convenience are sufficient to encourage consumers to participate in e-commerce. Consumer trust in the online world cannot be separated from the future of e-commerce.

In future related research we will consider how effective existing security schemes for e-commerce transactions (notably SSL and SET) are in addressing consumer concerns. This will lead to a better understanding of how best to approach e-commerce security issues from the perspective of promoting greater consumer involvement in e-commerce.

REFERENCES

Bhatnagar, A., Misra, S., and Rao, H. R. (2000). On risk, convenience, and internet shopping behaviour. *Communications of the ACM* , **43**(11), pp. 98–106.

BS 7799-1 (1999). *Information security management — Part 1:Code of practice for information security management*, British Standards Institution.

Burnett, S. and Paine, S. (2001). *RSA Security 's Official Guide to Cryptography*. Osborne/McGraw-Hill.

Caldwell, K. (2000). Global electronic commerce – moving forward. *CommerceNet: The Public Policy Report*, **2**(11), pp. 2–17.

Friedman, M., Kahn, P. H., and Howe, D. C. (2000). Trust online. *Communications of the ACM*, **43**(12), pp. 34–40.

Ghosh, A. K. (1998). *E-Commerce Security, Weak Links, Best Defences*, John Wiley and Sons.

Hassler, V. (2000). *Security Fundamentals for E-Commerce*, Artech House.

ISO/IEC 17799 (2000). *Information technology — Code of practice for information security management*, International Organization for Standardization, (http://www.iso.ch).

Oppliger, R. (2000). *Security Technologies for the World Wide Web*, Artech House. House.

Schneier, B. (2000). *Secrets and Lies*, John Wiley and Sons.

Stein, L. D. (1998). *Web Security*. Addison-Wesley.

Tomlinson, M. (2000). Tackling e-commerce security issues head on. *Computer Fraud and Security*, **2000**(11), pp. 10–13.