Conflicting Consumer's myth on security and privacy in E commerce

P. S. Nagarajan
Assistant Professor, Alagappa Institute of Management,
Alagappa University, Karaikudi.

J. Ashokkumar
Research Scholar, Alagappa Institute of Management,
Alagappa University, Karaikudi.

Abstract

Web security has been a major issue of debate in the recent years. The lack of security is perceived as a major obstacle for doing business online. Electronic cash payment systems are becoming more important than ever to facilitate online transactions and thus replacing traditional payment methods such as cheques. The prime objective of this paper is to determine the perception of consumers towards the security aspects of e-commerce technology. Specifically this paper discusses the perception and awareness of security from the consumers' standpoint in recent e-business processes and its related activities that facilitate transfer of payment via electronic systems such as e-wallet, credit card and e-cash. The paper also examines the measures that can be taken, so that the mindset of users can be changed to suit this new on-line culture. This modern concept would be divulged with the rural consumers, the rural consumer could hence avail the facilities through the modern technologies with secured manner.

Keywords*: consumer perception, security, privacy, E commerce.*

Introduction

The information revolution has provided part of the world's population with advanced information superhighway that we know as the Internet. Use of the Internet for on-line purchases and some transactions forms just part of the growth in global electronic commerce (e-commerce), which is actually a broader use of information technology by businesses and the government. Its revenues are projected to reach US$152 billion this year in Europe, and the global revenue from e-commerce in Europe, US and Japan achieved a total of US$657 billion in 1997. In 2002, the global figure for e commerce projected was to reach US$1,500 billion. The potential growth for e-commerce in Malaysia still remains huge. From a modest RM12.5 million in on line sales in 1997, Malaysia was projected to achieve over RM647 million in online sales in 2002.

However, the users remain extremely concerned about the level of privacy and security of this technology. Rapid growth generally brings about several concerns. One survey conducted showed that only one third of all local Internet users have made online purchases in 2001. A recent survey result also indicated that 70% of corporate purchasing decision-makers indicated that security concerns hindered them from buying over the Internet. Another general survey among individuals of general public, to determine people's attitude towards security showed that, 58% who had not yet purchased online cited insecure communications (51%), potential untrustworthiness of the vendors (43%) and no need to buy online (46%) as their concerns towards e-commerce. According to the independent research firm forester, Total ecommerce revenue in India is expected increase by more than five times

by 2016, from US$1.6 billion in 2012 to US$8.8 billion in 2016. In the venture capitalists invested $177 million in ecommerce in India.

Objectives

Security issues emerge as the utmost concern in the mind of the consumer. Besides that, there are many Threats in e-commerce, for example intellectual property threats, client threats, communication channel threats, viruses and server threats. Security plays a very important role in overcoming these threats. Failure of overcoming these threats will cause a negative impact not only to the e-commerce businessman but the consumers as well. Security will become an obstacle to the development of e commerce when people take it lightly.

Business and retail transactions move into a new era leveraging on the electronic platform, namely the Internet. Many traditional businesses are considering electronic commerce as a lucrative alternative mode for exchange of transactions. Though e-commerce is widely spoken and also predicted as the new way of doing business transactions, it however, had failed to attract significant number of customers. Many consumers due to security issues claimed that they simply do not prefer purchasing goods and services via the Internet. Therefore the aim of this paper is to find out the perception of consumers towards issues in e-commerce, particularly on security and privacy. The research questions are: (1) what is the customer's perception towards ecommerce security today? And (2) how can we change the consumer's perception on security issues?

Review of Literature

Hudgins and Christy (1998) stated that the rapid growth of e-commerce has attracted a lot of commerce service provider (CSP) company to be set up worldwide. However, the little knowledge and primitive ideas about what constitutes good security has caused concern to people. For example, some CSPs transmit credit-card information without any form of encryption, some only use a single firewall while some never use at all but only rely on the filtering of their routers. This may cause some risk to the company as well. He explained that ecommerce merchants need to ensure that encryption occurs in their credit-card transactions with the consumer, as well as in any back-end transactions that credit-card information or directly to the merchant. He described that it is ideal to have physical security and logical security together. This article only describes the implementation of security in e-commerce. The impact of the poor security control on e-commerce and consumers are also not described.

Chadwick (2001) stated that creating trust is one of the processes in building a relationship with a consumer. He mentioned that research showed that trust could develop over time or swiftly. He explained that there is a difference between e-commerce interactions and face-to-face interactions in the process of building relationship with a consumer. He stated that trust must exist for a successful transaction. He described that trust does affect how consumer can behaves in an e-commerce transaction. When the price differences are small, consumers preferred to buy from an online company they trust. He also explained that trust problem appeared both in e businesses and consumers.

According to a survey conducted by Chew (2003), 77% (653) of the 852 respondents from major towns in all the states of Malaysia used the Internet. From these 653 respondents, 12% of them used the Internet to buy items related to their work, 7% of them used the Internet to sell items related to their work, 17% of them used the Internet for banking transactions, 13% of them used the Internet to pay bills and 10% of them have bought some product through the Internet in the last 12 months. The findings also showed that they are not confident to transfer money, give their credit card and personal information through the Internet. They also agreed to use the Internet as a medium of transaction if they can be sure that their credit card will not be overcharged. However, the respondents generally neither agree nor disagree when it comes to the belief that their personal information will be sold to other merchants without their consent when buying through the Internet. Since they are not confident to give their personal information through the Internet, it is expected that one of the possible reasons is that personal information will be sold to other merchants without their consent when buying through the Internet. However, this seems to be not a reason. The limitation of this study is that it did not give reasons as to why their confidence level on the Internet is low when it comes to transferring money, giving their credit card and personal information through the Internet. Lack of trust on Internet security could be a reason. Another reason could be that the Internet users do not trust online merchants to behave ethically where money and customers‟ information is concerned.

The promotion and optimum use of security, privacy and trustworthiness are important elements for supporting the growth of business-to-consumer e-commerce. Two problems with existing e-commerce literature include the extent to which privacy and security issues are conceptualized as distinct, and the lack of understanding of how they are related. As illustrated in the 2012. Harris Interactive poll discussed. Another common practice in the literature is to use global terms such as safeguard assurances to represent both privacy and security concerns. This conceptual confusion is often followed by discussions of which type (privacy and/or security) of Web features maximally reduce consumer fears, in addition to how to place and convey these features on the site.

Main Security Threats

Online Credit Card Fraud

One major cause of consumer dilemma is the usage of credit card over the Internet. Credit card to a certain extent portrays the following threats:

- When an Internet vendor detects fraudulent credit card information, the credit card cannot be confiscated and the fraudster and credit card are free to try alternative sites.
- Fraud perpetrators are also free to use stolen card numbers or even attempt to manufacture numbers for use, as purchase over the Internet does not need the actual cards and signature.

- The remoteness of the buyer and seller make it extremely difficult to apprehend the fraud perpetrator. In fact, remoteness is among the factors that attract individuals to electronic commerce fraud.

Privacy

Hackers breaching sophisticated systems have become more common these days. It is performed by means of identifying passwords, breaching firewalls and with other hacking tools. Besides, they don't need sophisticated understanding of the computers and Internet to crack a company's computer. ID numbers, passwords, credit card numbers and fraud instruction guides are available in Internet chat rooms.

Applications Corp claims that many electronic commerce sites do not adequately protect consumer's databases and are vulnerable to hackers seeking customer information (Morgan, 1999). However, there are other sources of threats from potential intruders like competitors, trading partners, employees or customers. Richard Powers of the Computer Security Institute single out competitors as the greatest threat in computer crime (Young, 1996). Competitors are a real hazard to companies engaging in electronic commerce as they try to steal valuable customer information. Besides, many web a server host computer that runs other servers besides the web server. One such example is the FTP server. This server sends and receives message in clear text. Yet, many organizations are using this method for transferring sensitive data or information between host computers and remote computers over the Internet. Thus, key passwords for sensitive directories are likely to be broadcast semi publicly over the Internet, where anyone with a little luck and packet sniffer can discover them.

Authentication

Domain Name System (DNS) spoofing is also possible with improperly set permissions. In DNS spoofing, hackers with write access changes the translation file rerouting web surfers to hacker.com. If the two WebPages look identical, even prudent customers can be easily defrauded and the company's reputation damaged.

Vulnerabilities in General Security Procedures

Security breaches takes place too often when security measures are bypassed. Carelessness like giving out passwords over the phone or throwing security manuals without shredding can create problems if it falls in the wrong hand. One important way to control the system security is by having a tight access control. That is by giving the users access only to their job functions and not more than that. Besides there should always be check and balance for the accesses granted. For instance, a data entry clerk should not be given access to delete the data, and there should be an independent checker to ensure the comprehensiveness and completeness of data.

Security System Design

Companies that don't adhere to good security designs are exposing themselves and the consumers' data to fraud. Good security design includes good general control, proper segregation of duties, clearly delineated lines of authority, internal audit, good documentation, proper authorization, internal audit and approval for both transaction and program changes. With all these measures in place, careful attention must be given to the prevention, detection and correction of security breaches.

Main Security Solutions

In line with the above mentioned security threat, security has always been the major concern of big players in e-commerce, regulatory bodies and also service and system providers. Online business requires a new type of security. Conventional security systems are designed to keep people out and limit access to important information and computing resources. But e-commerce requires security systems that give authorized outsiders access to crucial company resources and applications, whether they're online payment systems, inventory data, or the ability to do transactions via the Internet. As the technology emerges, the following techniques have been developed to tighten up security. Again, the issue here is how far the consumers are aware of these technologies. A few technology methods to overcome the Internet security threats are listed below.

Encryption

Sensitive information such as credit card details can be defended by encryption, that is, the use of secret codes. The goal of encryption is to make it impossible for a hacker who obtains the *cipher text* (unreadable form of the message after being encrypted) as it passes through the network, to recover the original message. Encryption is the mutation of meaningful information in any form into a form that can only be rendered readable by a *decryption key*. There are two main types of encryption in common use today – symmetric, or private key systems and asymmetric or public key systems. In a symmetric key system, the same key is used to encrypt and decrypt the plaintext. The key is called a private key and must be shared by the sender and receiver of the text.

Public-key encryption uses two closely related keys. One key is used to encrypt the message, and the other key is used to decrypt the message. This works because the two keys are mathematically related in such a way that data encrypted with one key (either key) can only be decrypted by using the other matching key. The public key can be made known to other parties, and can be distributed freely. The private key must be kept confidential, and *must be known only to its owner*. Both keys, however, need to be protected against the slightest modification, or the mechanism will not work.

The best-known public-key encryption *algorithm* is RSA (named after its inventors Rivest, Shamir and Adleman), and now the property of RSA Security Inc. (In this context, an algorithm is a step-wise mathematical encoding process that converts original data into the

stream of encrypted data i.e. the hypertext). The 'secret to success' of this process is that: whatever data that one of the keys ‘locks’; only the other key of the pair can 'unlock'. Also, *technically*, it does not matter which of the keys performs the encryption – it is *only the other key of the pair* that can perform the decryption. In practice however, it is very important, in every e-commerce situation, to decide which of the pair of keys should be used to perform the encryption or the decryption, depending upon the circumstances involved.

Kalakota and Whinston (1997) gave an example that illustrates the use of public-key encryption: "... if an individual wants to send a snoop-proof email message to a friend, she simply looks up *his* public key and uses that key to encrypt her text. When the friend receives the email, he uses his private key to convert the encrypted message on his computer screen back to the sender's original message in clear text." Since the text was encrypted using the *receiver's* public key, the *only* key that can decrypt the data is the *receiver's private key*, thus ensuring that this person is the only one who can read the message, even though it may have been intercepted en route by other unauthorized recipients. Even if a would-be criminal gains access to the message along the way, it cannot be decrypted without the private key.

Public-key encryption is very useful when the parties wishing to communicate securely cannot rely on each other to maintain confidentiality, or do not share identical 'secret' keys. Clearly, this is often the situation in online commerce, and especially in Business to consumer (B2C) e-commerce, where many customers need to communicate securely with a single virtual store. Another prominent aid to this method is the use of *digital signatures*.

Digital Signature

A digital signature is a cryptographic method that fulfils a similar purpose, as does a written signature. It is used to identify and verify the originator and the contents of a message. That is, a recipient of data (such as an email message) can verify who signed the data, and that the data was not modified after being signed. The main purpose of digital signatures is for sender authentication. In fulfilling this goal, the mechanism is such that the sender cannot repudiate having (digitally) signed the data. It also enables the computer to annotate the message, ensuring the recipient that the message has not been forged ('spoofed') in transit by another person.

Digital Certificate

Authentication is further strengthened by the use of *digital certificates*. Digital certificates verify that the holder of a public and private key is who they claim to be. Third parties called certificate authorities (CA) issue digital certificates. Most certificates follow the Internet Engineering Task Force’s (IETF) X.509 certificate standard. Under version 3.0 of this standard, a certificate contains items such as the subject’s name (owner of the private key), validity period, subject’s public key information and a signed hash of the certificate data (i.e. hashed contents of the certificate signed with the CA‟s private key). Certificates are

used to authenticate Web sites (site certificates), individuals (personal certificates) and software companies (software publisher certificates) There are a growing number of third party CA's. VeriSign (verisign.com) is the best known of the CAs. VeriSign issues three classes of certificates. Class 1 verifies that an e-mail actually comes from the user's address. Class 2 checks the user's identity against a commercial credit database. Class 3 needs notarized documents. Companies like Microsoft offer systems that allow companies to issue their own private, in-house certificates. These can be used to identify users on their own networks (Turban *et. al*, 2002).

Netscape introduced SSL with its Navigator Version 2.0 browser, and Microsoft has included it in its line of Internet Explorer browsers since that time. It addresses some of the security concerns relating to data transfer over the Web. The Web itself, because it uses simple TCP (Transmission Control Protocol) for its transmission process, does not encrypt the data sent across it. Anyone who intercepts a Web transmission has complete access to the data contained therein. If a transmission containing credit card numbers falls into the wrong hands, it is important that this data should not be readable by anyone other than the sender and the intended recipient. Enter SSL, which works in the following way: When a user sends data via a mechanism displayed by a web browser (e.g. a shopping carts order form), the data is formatted to conform to the HTTP (Hypertext Transport Protocol) protocol. The necessary data transfer commands, together with the order data itself, are sent and received through connections called *sockets* that enable two remote computers to talk to each other via the Internet. The problem with this is that most of the transmission is done in the plain text that can be read by almost anyone having access to this data. SSL solves this by automatically encrypting the content component of HTTP transmissions before it is transmitted, and then decrypting the data at the receiving end, using the appropriate decryption key.

Like all public-key encryption systems, SSL security hinges on the difficulty of unlocking an encrypted message without the key. Assuming that the underlying algorithm is mathematically secure, the difficulty involved in 'cracking' an encrypted SSL message is a function of the key length. If the key is only 8 bits long, for example, messages would be easily decipherable because 8 bits allows only 'two to the-eighth', or 256 unique permutations of possible keys. Any computer could arrive at a solution very quickly by trying all 256 keys in succession. On the other hand, a key-length of 512 bits (called 'military-strength' encryption) would present a formidable obstacle. With 'two-to-the-512' possible keys to try, a supercomputer capable of testing one million keys per second would require centuries to find the correct key to unlock the encrypted message. Most e-commerce websites employing SSL are now using 128-bit keys, and this is called *strong Encryption.* For most e-commerce purposes, this key length ensures a level of security that might as well be called "absolutely secure", as far as transaction security is concerned.

Secure Electronic Transaction (SET)

According to Turban *et al*. (2002), SET is a cryptographic protocol designed to handle a complete transaction. It is developed by Visa and MasterCard. There are 3 entities in a SET

transaction – customer, merchant and payment processing firm. SET use SET digital certificates for each of these entities to ensure mutual authentication. When a customer wants to make a purchase, he uses an electronic wallet. An e-wallet is a helper application used to store information about the customer's credit cards and the SET digital certificates for each of the cards. The e-wallet sends both the order information and the payment.

Encryption is the application of a mathematical algorithm to a message in order to scramble that message. The recipient must have the decrypting key to unscramble the message. Secure socket layer (SSL) technology is present in most modern Internet browsers, and encrypts information so that it is difficult to view the information without the authorized key. Secure electronic transaction (SET) is another encryption technology that additionally uses a certificate authority to apply the key for decryption and protects credit information by allowing only the payment clearinghouse, not the merchant, to view such information. The use of these technologies greatly decreases the opportunity for unauthorized access to information passed over the Internet.

The former is encrypted with the merchant public key and the latter with the payment processing firm's Public key. Therefore, the payment-processing firm cannot see the order information and the merchant cannot see the payment information. In addition to securing orders and payments, SET also supports the following features such as cardholder registration, merchant registration, purchase requests, payment authorizations, payment capture, credits, credits reversals and debit card transactions. The acceptance of SET is very slow.

The major problems are that SET

- Requires specialized software for both the client and server.
- Slower than SSL
- Has a higher associated transaction cost?

Conclusion

Online sales offerings from e-commerce firms have the potential of fundamentally changing the way Consumers purchase goods and services. However, the potential of e-commerce has not been fulfilled due to consumer's perceptions of the risks involved in conducting business online. It covers the issues concerning security and privacy while doing online transactions. There are a lot of literatures to prove that the technological aspects in ecommerce focusing on security and privacy are safe and sound but the consumers still perceive that they are not enough and show dissatisfaction. We are trying to discuss through literature that it is the perception of the consumers that stops them from using e-commerce. Security is an issue not only to consumers but also a concern to programmers and administrators.

They face the problem of losing valid data and intrusion of viruses. E-commerce sites must address Internet customers' concerns over security and privacy. In addition to designing sites for ease of use, usability specialists can expand their role by understanding how to study

consumers' perceptions of security, privacy, and trust. When it comes to consumers, they should be aware of various security loopholes and learn how to manage and prevent security threats. They should learn how to overcome the antecedents of security and privacy. Along with the Internet security problems, businesses also must address the problem of fraudulent activity conducted over the Internet. Although the fear of Internet fraud tends to exceed the incidence of harm, the problem is nevertheless very real. Even exaggerated perceptions of risk have the potential to hinder online commerce. Finally the paper concludes that there should be more literature to educate consumers and bring awareness to them. A lot of literatures are needed to find out how risk perceptions influence e-commerce, how retailers manage it and how the management of risk perceptions may impact consumer welfare. In order to increase the confidence among consumers about the perception on Internet security issues, the following are guidelines that our paper recommends:

- Consumers must educate themselves to protect their confidential information and consumer rights.
- Poor usage of passwords is another reason for security breaches. Users or staff in organizations may not use strong passwords because it is not easy to remember. Four character passwords are too easy to guess. Six to eight character passwords are more difficult to crack. Examples of strong passwords are “dog% sky”, “24tohh4s21”.
- There are many passwords guessing programs publicly available with built in dictionaries containing hundreds and thousands of words so users must be careful.
- Consumers should be more proactive to know the sites they are visiting and be more cautious in giving personal or financial information and also take the effort to know the credibility of the organization they are dealing with.
- Internet Security and Consumer Rights courses are to be made available in secondary education system. Citizens should be taught about these issues when they are young.
- IT and Internet Security Road shows and Exhibitions to be extended to rural areas to educate the rural people.
- PC Ownership campaigns to be extended to have more citizens to access the Internet and learn about E commerce and Internet Security.
- Self-regulation by the industry, since the laws in India and other parts of the world are quite vague.
- Educate them as to how their personal data can be protected.
- Understand consumer rights and deficiencies of the law.

References

1. Foresight (1998), “E-commerce Sets New Rules,” *Systems Relationship Marketing,* on behalf of Datatec Ltd, Vol. 1 No. 3, November.
2. Morgan, C. (1999), Protecting Your Website against Credit Card Fraud. *Computerworld,* p.71.
3. Young, J., Spies like us. *Forbes,* June 3, 1996, pp. 70-92
4. Chokani.S and Ford, W., Internet Public Key Infrastructure Certificate Policy and Certification practices Statement Framework, Internet Draft, September, 1997

5. Greenwich, Conn.-IVANS (Insurance Value Added Network Services) source:www.ivans.comMcKeefry. www.ebnonline.com/supplements/extras/story/OEG20000406S0006
6. Chew, K.W., (2003) "*To Determine the Readiness of Business Entities and Consumers for A Successful Implementation of Electronic Commerce in Malaysia*" End-of –Project Report submitted to the Ministry of Science, Technology and the Environment, Malaysia.
7. Julie,B(1997)., http://disc.cba.uh.edu/~rhirsch/fall96/barba.htm
8. Portz *et al* (2000) http://uwstudentfpweb.uwyo.edu/J/JP/WebTrust.htm
9. Ramsey and eMarketer -www.newsfactor.com/perl/story/6530.html
10. Chadwick,S.A., http://chadwick.jlmc.iastate.edu/
11. Electronic Commerce, Second Annual Edition, Gary P. Scheneider and James T. Perry, p3
12. Bonafield, C.H., (1998), Cashing In on E-Commerce. Network Computing.
13. Miyazaki, Anthony D. and Fernandez, A., (2000), "Internet Privacy and Security: An Examination of Online Retailer Disclosures," *Journal of Public Policy and Marketing*, 19 (spring), 54-61.
14. Kalakota, R and. Whinston, A. B. (1997). *Electronic Commerce: A Manager's Guide.* Addison Wesley.
15. Turban, E., King, D., Lee, J., Warkentin, M. and Chung, H.M. (2002*) Electronic Commerce: A Managerial Perspective 2002*, Prentice Hall, USA.