Building consumers' confidence in adopting e-commerce: a Malaysian case

Mohiuddin Ahmed

Kulliyyah of Information and Communication Technology,
Department of Computer Science,
International Islamic University Malaysia,
P.O. Box 10, Kuala Lumpur 50728, Malaysia
E-mail: mohiudin@iiu.edu.my

Ramlah Hussein and Rashidah Minakhatun

Kulliyyah of Information and Communication Technology,
Department of Information Systems,
International Islamic University Malaysia,
P.O. Box 10, Kuala Lumpur 50728, Malaysia
E-mail: ramlah@iiu.edu.my
E-mail: yi_thaw@iiu.edu.my

Rafikul Islam*

Kulliyyah of Economics and Management Sciences,
Department of Business Administration,
International Islamic University Malaysia,
P.O. Box 10, Kuala Lumpur 50728, Malaysia
E-mail: rislam@iiu.edu.my
*Corresponding author

Abstract: Consumers' confidence on the online transactions is vital for the continuous growth and development of electronic commerce. In this study, we experimentally investigate the measures of consumers' perceived security and privacy over online transactions as well as the perceived trust and reliability of online vendors in order to influence consumers' overall confidence in e-commerce transactions. On the basis of responses from 163 participants, it is concluded that the major concerns in e-commerce adoption are: security and privacy over online transaction process and trust and reliability of online vendors. In order to be successful in electronic marketplace, the organisations are expected to expend their resources and exert efforts to ensure that consumers' concerns are adequately addressed.

Keywords: e-commerce; security and privacy; trust; online vendors; consumer behaviour; Malaysia.

Reference to this paper should be made as follows: Ahmed, M., Hussein, R., Minakhatun, R. and Islam, R. (2007) 'Building consumers' confidence in adopting e-commerce: a Malaysian case', *Int. J. Business and Systems Research*, Vol. 1, No. 2, pp.236–255.

Biographical notes: Mohiuddin Ahmed is an Assistant Professor in the Department of Computer Science at International Islamic University Malaysia (IIUM). Before joining IIUM, he was working in Goldman Sachs, NY, USA, as a Programmer Analyst in Global Control Division. Prior to that, he was an Adjunct Faculty in the Department of Electrical and Computer Engineering in North Carolina A and T State University (NC A and T SU). He received an MS and PhD both in Electrical Engineering from NC A and T SU, USA in the year 1993 and 2000, respectively. His current research interests include high performance computing (HPC), artificial neural network (ANN), ANN application in signal and image processing, etc.

Ramlah Hussein is a BSc in Systems Science (Business) at the University of West Florida. After graduation, she became a Lecturer at Universiti Teknologi Malaysia. She pursued her Masters degree at Universiti Technologi Malaysia and graduated with MSc in Technology Management in 1996. She completed a PhD in Management Information Systems at University Putra Malaysia in 2005. She has more than 10 years of teaching and research experience in public and private institutions. Currently, she is an Assistant Professor at the International Islamic University Malaysia (IIUM). Her research interests cover areas related to IS effectiveness, organisational and technological issues in IS and e-government related studies.

Rashidah Minakhatun is currently a postgraduate student at the Department of Information Systems under the Faculty of Information and Communication Technology, International Islamic University Malaysia. She received a Bachelor of Management Information System (Honours) from International Islamic University Malaysia in 2004. Her research interests include the internet security, privacy and e-commerce.

Rafikul Islam received an MSc in Applied Mathematics from Calcutta University in 1988. Subsequently, he received a PhD in Operations Research from Indian Institute of Technology, Kharagpur in 1996. Presently he is working as a Professor at the Department of Business Administration, International Islamic University Malaysia. His papers have appeared in *European Journal of Operational Research, Military Operations Research, Journal of Engineering Manufacture, Journal of International Business and Entrepreneurship Development, International Journal of Business Information Systems, IIUM Journal of Economics and Management*, etc. His research area includes multiple criteria decision-making, operations and quality management.

1 Introduction

One of the major areas that is significantly affected by internet today is the way people buy and sell products and services in the competitive market. By virtue of internet, e-commerce has been the counter part of the traditional brick and mortar business. E-commerce is the process of buying, selling or exchanging products, services and information via communication networks such as the internet, intranet and extranet (Turban and King, 2003). With the advancement of the internet, we can order books, cloths, appliances and gifts online, book a hotel room across the ocean, check our credit card and bank balances 24 hr a day or access our offices from thousands of miles away.

Even though e-commerce is spreading worldwide, many customers are still reluctant to deal with it because of the security and privacy concerns (Ahuja et al., 2003; Basu and Muylle, 2003; Bingi et al., 2000). While the internet helps make our lives richer and more convenient, it also provides a gateway to access our personal information. Many consumers feel that their personal information may be disclosed to others without their knowledge. Furthermore, viruses, hackers, crackers and worms have become the stuff of headlines with results that range from mere headache to a complete disaster. It is generally recognised that security measures are extremely important for e-commerce and all e-businesses running on the internet. According to Braithwaite (2002), e-commerce security can be addressed by paying more attention to how business information is collected and handled, how hardware and software process and communicate that information, and how system resources are configured and made safe to ensure its availability to only legitimate users.

A number of research findings (Basu and Muylle, 2003; Heuvelmans, 2000) confirm that consumers' adoption of electronic transactions on the web is growing at a lower pace than expected because consumers do not simply trust most sites on the internet today to furnish personal information that involves money. This means that, despite the internet-based electronic transactions offer many opportunities and promises to consumers, the number of consumers making online purchases are still few compared to the total number of people browsing the web. Concerns about security, trust, authentication, fraud and risk of losing money are often cited among the significant barriers in the growth of e-commerce.

This paper intends to identify the factors which are directly related to Malaysian consumers' confidence to adopt e-commerce. In the last few years, there has been significant increase in e-commerce activities in Malaysia. In 2000, 3.7 million people in Malaysia (15% of the total population) subscribed internet and the figure rose to 10.1 million (37.9% of the total population) in 2005. Further, according to Lincoln Lee, Senior Analyst, Telecommunications Research, Malaysian e-commerce market is expected to grow by the margin of 70.1% in 2006 in comparison with that in 2005. Some of the initiatives taken by the Malaysian government to promote e-commerce are: introduction of cyber laws and intellectual property laws, building nationwide telecommunications infrastructure and services, enhancing e-payment systems and above all launching the super project called 'Multimedia Super Corridor' (Paynter and Lim, 2001).

Specifically, the objectives of the present research are the following:

- to investigate whether or not consumers' perceived security and privacy of online transaction and also their personal information significantly affect their confidence to adopt e-commerce
- to investigate consumers' perception on whether or not there is an adequate control in place to protect the security and privacy of consumers' personal information within merchant systems
- to identify the factors of trust with online vendors to engage in transactions involving money and personal information.

A brief account of some of the recent and relevant literature is provided in the next section.

2 Literature review

Internet has created enormous change in the business environment. Systems are devised to facilitate Business-to-Business (B2B), Business-to-Customer (B2C), Business-to-Government (B2G), Government-to-Citizen (G2C) and so on. Private communication networks and the internet are being increasingly used by organisations to establish corporate alliances with suppliers, business partners and customers. Porter (2001) mentioned that an organisation could gain two types of benefits from the internet: operational efficiency and strategic positioning. Blount et al. (2005) argued that all competitors are capable of achieving operational efficiency in time. It is only strategic positioning that can deliver sustainable competitive advantage. The authors described how two banks in Australia linked their e-commerce strategies with their overall business strategies and the extent to which their HRM strategies have helped them utilise their e-commerce capability to achieve sustainable competitive advantage.

As it is mentioned earlier, consumers' adoption of e-commerce is growing at a lower pace than expected. For example, the Small- and Medium-Sized Industries Association of Malaysia said in late 2005 that less than 5% of its members were involved in B2C business. Furthermore, according to mid-2005 survey conducted by the Malaysian Communications Multimedia Commission (MCMC), only 9.3% of internet users had purchased products or services through the internet during the preceding three months (Economist Intelligence Unit, 2006). The primary reasons cited for this are: lack of security and privacy of consumers' personal data including credit card number, identity theft, virus, break-in attacks, denial-of-service, etc. An identity thief steals key pieces of personal information and uses it to impersonate someone and commits crimes in his/her name and it is regarded as the fastest growing internet crime today (Sorbel, 2003). The ability to know the identity of the person or the business enterprise with whom we are doing business is important. Thus, authentication services are fundamental to achieving secured e-commerce. Basu and Muylle (2003) have evaluated 17 currently available authentication mechanisms in e-commerce using six criteria, namely, robustness, acceptance, cost, ease of use, portability and security. Koch and Möslein (2005) feel the need for user-centric global identity management in e-commerce.

In the earlier days of the internet, people were obsessed with the notion that hackers could capture credit card numbers while these are transmitted through the internet. As a result, merchants paid more attention on protecting credit card data by ensuring that it was not transmitted in its original form, by encrypting it so that it could travel securely over the internet. However, in reality, most security breaches occur after the transaction is completed. It means when a customer's credit card number is kept unprotected in merchant's computer, the possibility of misuse is more. In this way, a hacker can net a file of several thousand credit card numbers. Therefore, protecting merchant's website is more important than securing the transactions through website at the time of the transaction (Sorbel, 2003).

A study of consumer-perceived risk in e-commerce transactions by Salam et al. (2003) indicates that consumers simply do not trust online vendors to engage in transactions that involve money and personal information. Trust is defined as confidence on the part of the trusting party that the party is reliable, has high integrity and is associated with such qualities as consistency, competency, honesty, fairness, responsibility, helpfulness and benevolence (Ghosh, 2001). According to the authors, consumer-perceived risk is reduced with the increase in institutional trust. Cheung and

Lee (2001) indicated that perceived security control and perceived privacy control are critical characteristics of online transactions affecting the development of online consumers' confidence on e-commerce. Salam et al. (2005) viewed trust as a complex social phenomenon reflecting technological, behavioural, social, psychological and organisational interactions among human and non-human (technological) agents. The authors write (p.77):

> Without taking a comprehensive view of how consumer trust evolves and how it relates to specific actions, the desire by businesses to establish trusting relationships with consumers is like grouping for a solution in the dark.

Ratnasingam and Phan (2003) emphasised interorganisational trust to bolster e-commerce participation. According to them, the key success factors in building B2B interorganisational trust are:

- following high quality standards and best business practices
- having good online customer support
- having competent employees with soft capabilities to develop and maintain B2B partnership trust
- following well-planned B2B collaborative strategies.

Head and Hassanein (2002) developed a model for online trust, which illustrates the phases of consumer online trust and outlines the necessary interactions between consumers, vendors and referees to progress from one trust phase to another. They also discussed the impact and influence of trusted third party referees and their seals-of-approval as mediators for building online consumer trust.

Molla and Licker (2005) propose a research model-based on Perceived Organisational Readiness (POER) and Perceived Environmental E-Readiness (PEER) that encompasses innovational, managerial, organisational and environmental characteristics as determinants of e-commerce adoption and institutionalisation. Through experimental investigation, the authors find that e-commerce adoption is explained more by POER than by PEER. The authors suggest that developing countries should pay more attention to both organisational and environmental consideration when making e-commerce adoption decisions. Grandon and Pearson (2004) identified the variables: organisational readiness, managerial productivity, external pressure, decision aids, compatibility and perceived usefulness that differentiate between adopters and non-adopters of e-commerce for SMEs in Chile.

Through an experimental investigation involving 36 business and governmental agencies in five Caribbean nations, Fraser and Wresch (2005) found that the companies experienced modest to significant successes in e-commerce but have been experiencing impacts from national characteristics such as factor conditions, demand conditions, support industries, firm strategy and government policy.

Javalgi et al. (2005) develop a framework that embraces key global driving forces and national policy forces impacting e-business readiness in the Asia-Pacific region through conceptualisation of the key global forces as primary drivers of e-business readiness and national policy drivers as enablers of e-business growth. By means of strategic map, the authors identify where various countries in the Asia-Pacific region are currently positioned in terms of their e-business readiness. The value of the strategic map lies in its ability to assist a country's leaders and key decision-makers to identify the

critical parameters that have become obstacles for e-commerce growth. The authors conclude that for the developing nations, enhancing awareness and public understanding about the benefits of e-commerce are extremely important and they recommend that Asia Pacific countries should concentrate on developing human capacity building, basic access to ICT, low cost hardware and software, the usage of local language and higher level of government facilitation.

Looi (2005) examines the effect of five factors, namely, competitive pressure, security, relative advantage, IT knowledge and government support, on the adoption of e-commerce among small and medium enterprises in Brunei Darussalam. The authors find that these factors explain more than 50% of the variation in SMEs adoption and in terms of relative importance the ranking of these factors is: competitive pressure, IT knowledge, relative advantage, security and government support. On the basis of the analysis of data collected from 84 HK-based SMEs, Ching and Ellis (2004) identified seven factors that are linked with e-commerce adoption by the SMEs: decision-maker's age, education level, cosmopolitan outlook, perceived compatibility, cost, customer pressure and the perceived relative advantages of the innovation. Hynes et al. (2006) think that the development of a long-term and sustainable e-commerce environment is of great importance to China's economy. The authors have identified the barriers of e-commerce in China through empirical research.

Krishnan (2006) found that the majority of Malaysians interested in e-commerce are males (66%) and males below 30 years (42%) is the largest individual group of Malaysians interested in e-commerce. Further, Sharifah (2003) noted that despite government's effort to continuously promote usage of ICT, usage is still very much limited to urban areas and the states that are relatively more developed. For example, Kuala Lumpur and Selangor residents form 40% of the internet subscribers of the whole nation.

Sulaiman (2000) assessed the status of e-commerce usage in Malaysia on the basis of five main business processes and activities, namely, marketing, advertising, customer support and service, order and delivery and payment. The author found security issues as the main barrier to the implementation of e-commerce. Organisations were reluctant to use e-commerce as they felt that the transactions conducted electronically were open to hackers and viruses, which were beyond their control.

Khatibi et al. (2003) mention that Malaysian e-commerce industry has not taken off as expected. By means of a survey of 222 Malaysian manufacturers, traders and service providers, the authors conclude that from the company's point of view, the main barriers of e-commerce adoption are:

- problems of keeping up and understanding the technology itself
- lack of trained manpower
- uncertainties with regard to its operations and regulations
- high switching costs.

In view of the above, the authors suggest that any policy that aims at promoting e-commerce should take the above factors into consideration.

Jawahitha (2004) has raised serious concern on the protection of Malaysian consumers dealing with e-commerce transactions. According to her, the existing laws pertaining to conventional businesses are not sufficient to address the issues in e-commerce. Malaysian government has already taken steps to pass new laws and to

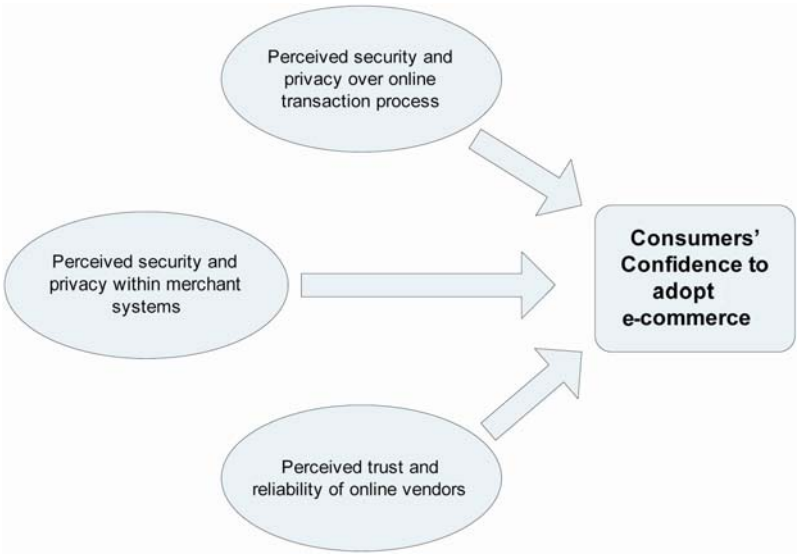
amend some of the existing laws and until this effort is materialised, the Malaysian electronic consumers would not be having adequate protection. To protect e-commerce consumers' privacy, Malaysian legislators have devised a personal data protection bill (Azmi, 2002). The author examines the nature, manner and scope of personal data protection under this Bill. She suggests that instead of being concerned with the full range of privacy and surveillance issues, the Bill deals only with the way personal data is collected, stored, used and accessed.

In essence, numerous research papers have been published during the last few years on various issues pertaining to e-commerce. Since this paper deals with building consumers' confidence in adopting e-commerce, it only cites literature relevant to the issue. In the last few paragraphs, a brief account of research on Malaysian e-commerce has been provided. As it is observed, in most of the surveys conducted in Malaysia, data have been collected from manufacturers/service providers. As far as the knowledge of the authors is concerned, so far no survey has been conducted in Malaysia involving consumers regarding identification of factors that help build their confidence in greater e-commerce participation. The present research is intended to fill-up this gap.

3 Research methodology

The objective of this research is to investigate the major factors that affect consumers' confidence to adopt e-commerce. The factors considered to be influencing consumers' confidence to adopt e-commerce are grouped into three main categories: consumers' attitudes towards online transaction processing system (Ahuja et al., 2003; Javalgi et al., 2005), security and privacy of consumer's personal information within merchant systems (Sipior et al., 2004) and trust and reliability of online vendors (Cheung and Lee, 2001; Salam et al., 2005). The model to be tested is shown in Figure 1.

Figure 1 Proposed research model that links various e-commerce factors with consumers' confidence



Specifically, the following hypotheses are to be tested:

H_1: Attitude towards secured online transaction processing system is positively related to the consumers' confidence to adopt e-commerce.

H_2: Attitude towards security and privacy of consumers' personal information is positively related to the consumers' confidence to adopt e-commerce.

H_3: Attitude towards trust and reliability of online vendors is positively related to the consumers' confidence to adopt e-commerce.

A questionnaire was designed that consisted of three sections. Section 1 consisted of questions to collect respondents' personal information, namely, gender, age, academic qualification, occupation, etc. Section 2 consisted of questions covering some of the variables related to electronic purchase and adoption of e-commerce. Specifically, the questions were designed to collect information on frequency of internet use, frequency of online purchases, intention to continue online purchasing, etc. Section 3 consisted of questions covering some of the variables related to factors affecting e-commerce security. Questions in this section collected information related to attitudes towards online transaction processing system, security and privacy of personal information and trust and reliability of online vendors. All the variables in this section employed Likert scale with endpoints ranging from 1 (strongly disagree) to 5 (strongly agree).

Before sending the questionnaires to the mass, it was pre and pilot tested. One PhD five Masters and four Undergraduate students were involved in the pretest. On the basis of pretest results, two questions were excluded as they were not directly related to the study. In addition to this, few statements in Section 3 were also rephrased. On the other hand, for the pilot test, the questionnaire was communicated to 50 non-academic staff from various departments of International Islamic University Malaysia (IIUM). Only 28 questionnaires were returned and on the basis of the results, few open ended questions were converted to statements that used Likert scale.

In the survey, the target group of respondents were the internet savvy employees who were working in various organisations in Malaysia. People contacted for this survey came from various professions: academic, banking, sales, management, administrative support, etc. Four hundred questionnaires were distributed upon personal contact with the respondents and they were requested to return the completed questionnaires later. However, only 182 completed questionnaires were returned. Respondents' profile has been shown in Table 1.

Table 1 Respondents' demographic information

Variable	*Frequency*	*Percent*
Gender		
• Male	68	41.7
• Female	95	58.3
Race		
• Malay	103	63.2
• Chinese	32	19.6
• Indian	14	8.6
• Others	14	8.6

Table 1 Respondents' demographic information (continued)

Variable	*Frequency*	*Percent*
Age group		
• 20–30 years	52	31.9
• 31–40 years	76	46.6
• 41–50 years	33	20.2
• 51 years and above	2	1.2
Highest level of education		
• High school	5	3.1
• Diploma	25	15.3
• Bachelors	63	38.7
• Masters	55	33.7
• PhD	11	6.7
• Others	4	2.5
Occupation*		
• Administrative Support	46	28.9
• Management	36	22.6
• Educator	19	11.9
• Sales personnel	10	6.3
• Professional	20	12.6
• Banking industry	51	32.1
• Others	14	8.8

*Respondents were asked to provide multiple occupations, if applicable.

4 Data analysis

As mentioned above, out of 400 questionnaires only 182 were returned and 19 of them were not usable due to incomplete information. Therefore, the analysis has been made based upon 163 usable questionnaires. As shown in Table 2, out of the 163 respondents, almost all the respondents (about 98.8%) report that they frequently use the internet while the remaining 1.8% do not use the internet at all. The table also shows that only about one quarter of the respondents make online purchases either sometimes or seldom even though the majority of the respondents frequently use the internet.

Table 2 Frequency of internet use and online purchasing

Response	*Internet use*		*Online purchase*	
	Frequency	*Percent*	*Frequency*	*Percent*
Always	93	57.1	0	0
Sometimes	65	39.9	23	14.1
Seldom	3	1.8	23	14.1
Never	2	1.2	117	71.8
Total	163	100	163	100

The respondents who made online purchases previously, were asked about how long they had been purchasing online. Out of 46 respondents who purchased online previously, about 10.9% have made purchases for less than one year, about 58.7% have made purchases between one and three years, about 28.3% have purchased between four and six years and about 2.2% have been purchasing for more than six years. Further, these respondents were also asked about the possibility of continued purchasing in the near future. About 4.3% of the respondents who purchased previously are willing to reduce their future purchases, while about 73.9% are willing to maintain the same status by neither increasing nor decreasing their online purchases. Also about 19.6% are willing to make a bit more purchases in the near future and only 2.2% are willing to make much more online purchases.

The respondents who did not have experience in online purchases were asked about the possibility of their willingness to make online purchases in the near future. Out of 117 respondents who never purchased online, about 82.8% are not willing to purchase in the near future and about 3.4% are willing to make online purchases in future. Furthermore, the respondents who never purchased previously and also who are not willing to purchase online in the near future were asked about the reason(s) for that. The major reason (57.7%) was cited to be the concern on security and privacy of their personal information. All the respondents were also asked about their opinion on credit card security for online purchases. The majority of the respondents (about 55.8%) believe that the use of credit card for online purchases is not safe, while about 20.2% believe somewhat safe. About 11.7% of the respondents are indifferent on online credit card security and the remaining (11%) respondents are not sure about this. The summary information of the foregoing analysis has been shown in Table 3.

Table 3 Summary of responses on various e-commerce issues

Issue	*Frequency*	*Percent*
How long have you been purchasing online?		
• Less than 1 year	5	10.9
• Between 1 and 3 years	27	58.7
• Between 4 and 6 years	13	28.3
• More than 6 years	1	2.2
Willingness to continue online purchases within the next six months (those who have experience in purchasing online)		
• I will not do this	0	0
• Somewhat less	2	4.3
• About the same	34	73.9
• Somewhat more	9	19.6
• Much more	1	2.2
Willingness to continue online purchases within the next six months (those who have experienced purchasing online)		
• I will not do this	96	82.8
• Somewhat less	4	3.4
• About the same	14	12.1
• Somewhat more	2	1.7
• Much more	0	0

Table 3 Summary of responses on various e-commerce issues (continued)

Issue	*Frequency*	*Percent*
Reasons for not buying online		
• Security/privacy	56	57.7
• Lack of time	8	8.2
• Lack of interaction	14	14.4
• Cannot feel product	13	13.4
• High price	6	6.2
Credit card security		
• Very unsafe	18	11.0
• Somewhat unsafe	73	44.8
• Indifferent	19	11.7
• Somewhat safe	33	20.2
• Very safe	2	1.2

4.1 Consumer attitudes towards e-commerce

4.1.1 Transaction processing system

Regarding online transaction processing system, about 27.7% of the respondents agree that the payment information they enter online is safe and accessible only by the intended persons (confidentiality) and only 9.9% of the respondents do not believe this. The remaining majority (62.3%) of the respondents remained indifferent to the question. On the integrity of the online transactions, only 8.6% of the respondents believe that the information they enter online is not altered in transit while 27.6% of the respondents do not believe this. The remaining majority (63.2%) of the respondents remained neutral on this question.

On the merchant authentication of the online transactions, only 4.9% of the respondents agree that all online vendors are those who say they are, while the majority of the respondents (about 73.6%) do not believe online vendors. About 21.5% of the respondents are not sure on this. On the issue of whether online vendors know that a consumer is a legitimate user of a valid account number during online transaction, approximately 20.2% of the respondents agree that merchant can know about the legitimate user of a valid account number while 19% of the respondents do not believe user authentication during online transaction and the remaining majority (60.7%) of the respondents remained neutral on this question. On non-repudiation, the majority of the respondents (about 74.2%) agree that the online transaction once confirmed cannot be abrogated later by either party, and only 6.1% do not agree on this and 19% of the respondents remained neutral on this question (see Table 4).

Table 4 Respondents' belief about online transaction processing systems

Response	*Confidentiality*		*Integrity*		*Merchant authentication*		*User authentication*		*Non-repudiation*	
	Freq.	*%*	*Freq.*	*%*	*Freq.*	*%*	*Freq.*	*%*	*Freq.*	*%*
St. disagree	0	0	1	0.6	18	11.0	1	0.6	2	1.2
Disagree	16	9.9	44	27.2	102	62.6	30	18.4	8	4.9
Neutral	101	62.3	103	63.6	35	21.5	99	60.7	31	19.1
Agree	43	26.5	12	7.4	8	4.9	33	20.2	104	64.2
St. agree	2	1.2	2	1.2	0	0	0	0	17	10.5
Total	162	100	162	100	163	100	163	100	162	100

4.1.2 Merchant system

Questions on attitude towards merchant systems are aimed at assessing the respondents' belief about protection of their personal information within merchant systems, whether the information entered online is safely kept in unreadable form and accessible only to the authorised personnel. About 46% of the respondents believe that there is an adequate control in place to protect the personal information within merchant systems, while only 6.7% do not agree on the security and privacy of personal information within merchant systems and 47.2% of the respondents remained indifferent to this question. As shown in Table 5, on the encryption of personal information within merchant systems, about 12.2% of the respondents believe that the information they enter online is safely kept in human unreadable form within merchant systems, while only 9.8% do not believe this; about 77.9% of the respondents are not sure whether their personal information is safely kept in human unreadable form within merchant systems. On access control, the majority of the respondents (about 65.6%) agree that the online vendors only allow authorised personnel to access confidential information in their systems; only 3.7% do not believe on access control, while the remaining 30.7% of the respondents were neutral on this question.

Table 5 Respondents' belief on merchant systems

Response	*Security and privacy*		*Encryption*		*Access control*	
	Freq.	*%*	*Freq.*	*%*	*Freq.*	*%*
St. disagree	1	0.6	1	0.6	2	1.2
Disagree	10	6.1	15	9.2	4	2.5
Neutral	77	47.2	127	77.9	50	30.7
Agree	75	46.0	18	11.0	106	65.0
St. agree	0	0	2	1.2	1	0.6
Total	163	100	163	100	163	100

4.1.3 Trust and reliability of online vendors

On attitude towards trust and reliability of online vendors, questions were aimed at assessing the respondents' belief about web vendors' trust and reliability on the use of consumers' personal information. Only 4.9% of all the respondents trust online vendors to engage transactions, while the majority of the respondents (about 79.8%) do not trust online vendors and about 15.3% of the respondents remained indifferent to this question. On the reliability of online vendors, only 2.5% believe that all online vendors are reliable. The majority of the respondents (about 82.9%) do not believe on the reliability of online vendors, while about 14.7% are not sure about this. Based on the responses as shown in Table 6, on the use of sensitive personal information, only 3.7% of the respondents believe that online vendors use the information entered online for intended purpose only, while about 18.4% do not believe about this and the majority (about 77.3%) of the respondents remained neutral on this question. On selling of personal information to third parties, only 4.3% of the respondents believe that online vendors will not sell personal information to third parties, while about 17.2% do not believe on this question and the majority of the respondents (about 78.5%) are not sure whether online vendors will sell personal information to third parties.

Table 6 Respondents' belief on online vendors and their confidence to adopt e-commerce

Response	*Trust*		*Reliability*		*Intended purpose only*		*Selling to third parties*		*Confidence in using complex method*		*Confidence for all necessary guarantees*	
	Freq.	*%*	*Freq.*	*%*	*Freq.*	*%*	*Freq.*	*%*	*Freq.*	*%*	*Freq.*	*%*
St. disagree	41	25.2	72	44.2	2	1.2	5	3.1	2	1.2	1	0.6
Disagree	89	54.6	63	38.7	28	17.3	23	14.1	4	2.5	3	1.8
Neutral	25	15.3	24	14.7	126	77.8	128	78.5	72	44.2	24	14.7
Agree	7	4.3	4	2.5	6	3.7	6	3.7	80	49.1	115	70.6
St. agree	1	0.6	0	0	0	0	1	0.6	5	3.1	20	12.3
Total	163	100	163	100	162	100	163	100	163	100	163	100

4.1.4 Adopting e-commerce

As shown in the last two columns of Table 6, on the use of more complex and advanced method to boost consumers' confidence to adopt e-commerce, the majority (about 52.2%) of the respondents agree that their confidence to purchase online will be increased when more complex and advanced method is used to address concerns on their security and privacy. And only about 3.7% do not agree on the use of more complex and advanced method and 44.2% of the respondents remained neutral on this question. On providing all necessary guarantees to increase consumers' confidence to adopt e-commerce, the majority of the respondents (about 82.9%) agree that their confidence to adopt e-commerce will increase when online vendors provide all necessary guarantees to ensure security and privacy of their personal data, while only 2.4% do not agree on this and the remaining (about 14.7%) respondents are not sure about this.

4.2 Factor analysis

Factor analysis (factor extraction as well as varimax factor rotation) was conducted to identify the underlying factors affecting consumers' confidence to adopt e-commerce. Considering all the 11 items on transaction processing system, merchant systems, trust and reliability of online vendors and consumers' confidence were analysed using principal component analysis. 'Total variance explained' (Table 7) shows the extent to which total variance of the observed variables is explained by each of the principal components. Initial factor extraction revealed four components with an absolute magnitude of eigenvalue greater than 1.0. The first principal component, which relates to the trust and reliability of online vendors and the largest part of the total variance, has an eigenvalue of 3.5 amounted to 31.9% of the total variance. The second principal component, which relates to the transaction processing system has an eigenvalue of about 1.8 and accounted for a further 16.27% of the total variance. The third principal component is related to the consumers' confidence to adopt e-commerce, has an eigenvalue of 1.2 amounted to 10.8% of the total variance. The fourth principal component has an eigenvalue of about one and accounted for 9.5% of the total variance. All the four principal components together accounted for 68.6% of the total variance in the original 11 items.

Table 7 Total variance explained

Component	*Eigenvalue*	*% of variance*	*Cumulative %*
1	3.509	31.898	31.898
2	1.790	16.273	48.172
3	1.193	10.848	59.020
4	1.048	9.530	68.550
5	0.777	7.063	75.613
6	0.633	5.758	81.371
7	0.581	5.279	86.650
8	0.485	4.413	91.063
9	0.413	3.751	94.814
10	0.340	3.088	97.902
11	0.231	2.098	100.000

Most items loaded onto the extracted factors except the items that were conceptualised to measure the attitude towards the merchant systems. Item on access control fairly loaded onto the factor of trust and reliability of online vendors, while the item on encryption slightly loaded onto the transaction processing system factor. However, items on user authentication of the transaction processing system fairly loaded onto factor one (trust and reliability of online vendors). Also items on merchant authentication and non-repudiation of the transaction processing system loaded onto factor four, as shown in Table 8.

Table 8 Results of factor extraction and factor loadings

Items in the scale	*Factor 1*	*Factor 2*	*Factor 3*	*Factor 4*
Intended purpose only	0.788			
Selling to other third parties	0.748			
User authentication	0.619			
Access control	0.549			
Confidentiality		0.821		
Integrity		0.809		
Encryption		0.693		
Confidence for complex and advanced method			0.862	
Confidence for all necessary guarantees			0.833	
Merchant authentication				0.729
Non-repudiation				0.669
Total initial eigenvalues	3.509	1.790	1.193	1.048
Percentage of variance	31.898	16.273	10.848	9.530

4.3 Reliability analysis

Reliability analysis was performed to assess the reliability of the scale used to measure the variables of interest. The overall reliability assessment of the entire scale was observed to be good with a Cronbach's alpha of 0.7062. A second test was conducted to assess the degree to which the items on the scale measure the hypothesised research constructs. A total of nine items measuring three constructs (four items measuring perceived trust and reliability of online vendors, three items measuring perceived security and privacy over online transaction processing system, and two items measuring consumers' confidence to adopt e-commerce) were assessed for reliability-based on item-to-total correlation criterion. As shown in Table 9, all nine items were observed to have item-to-total correlation of above 0.35. Assuming 0.35 as the cut-off value of item-to-total correlation coefficient, all items were included for further analysis.

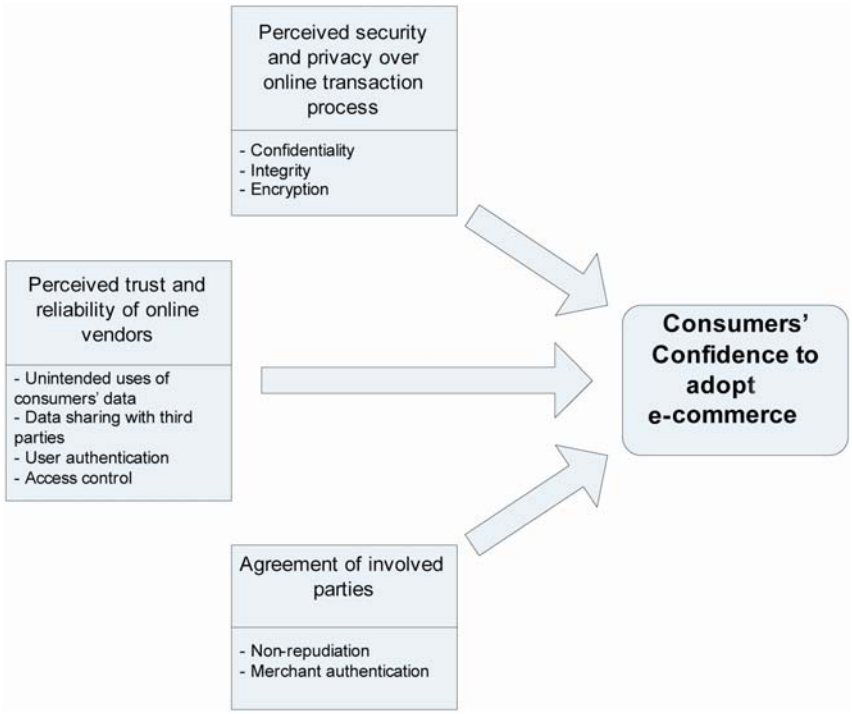
4.4 Hypothesis testing

The proposed research model discussed in methodology section has been modified-based upon the results of factor analysis. As shown in Figure 2, the modified constructs from factor analysis are perceived security and privacy over online transaction process, perceived trust and reliability of online vendors and agreement with involved parties. The variables under various constructs are shown in Figure 2.

Table 9 Reliability analysis results

Items in the scale	*Means and SD*	*Item-to-total correlation*	*Alpha*
Attitudes towards trust and reliability of online vendors			
• Intended purpose only	2.84 (0.48)	0.6257	
• Selling to other third parties	2.85 (0.55)	0.4498	
• User authentication	3.01 (0.64)	0.4045	
• Access control	3.61 (0.61)	0.4588	0.6905
Attitudes towards online transaction processing system			
• Confidentiality	3.19 (0.62)	0.5845	
• Integrity	2.81 (0.62)	0.5791	
• Encryption	3.03 (0.53)	0.4511	0.7152
Consumers' confidence to adopt e-commerce			
• Confidence for complex and advanced method	3.50 (0.66)	0.5878	
• Confidence for all necessary guarantee	3.92 (0.63)	0.5878	0.7398
Agreement of involved parties			
• Merchant authentication	2.20 (0.70)	0.7800	
• Non-repudiation	3.78 (0.75)	0.4212	0.2250

Figure 2 Modified e-commerce model for the present research



Pearson correlation coefficients were computed in order to test the relationships between each factor and consumers' confidence to adopt e-commerce.

> *H_1: Attitude towards secured online transaction processing system is positively related to the consumers' confidence to adopt e-commerce.*

The correlation coefficient between consumers' attitude towards secured online transaction processing system and their confidence to adopt e-commerce was found to be 0.173 with $p = 0.027$. Therefore, the research hypothesis is accepted.

> *H_2: Attitude towards trust and reliability of online vendors is positively related to the consumers' confidence to adopt e-commerce.*

The results of this study show that perceived trust and reliability of online vendors positively affects the consumer's confidence to adopt e-commerce ($r = 0.371$). The relationship is observed to be statistically significant with significance level less than 0.01 ($p = 0.000$). Therefore, we accept the research hypothesis.

> *H_3: Attitude towards agreement of involved parties is positively related to the consumers' confidence to adopt e-commerce.*

Here, we also find positive correlation coefficient of 0.362 with $p = 0.000$. Therefore, consumers' confidence to adopt e-commerce is positively related with their attitude towards agreement of involved parties.

Items related to the trust and reliability of online vendors such as unintended uses of consumers' sensitive data, data sharing with third parties, user authentication and access control of consumers' personal information were observed to be highly influential in the case of online purchases. Attitudes towards agreement of involved parties such as merchant authentication and non-repudiation were observed to be second most influential factors for e-commerce transaction followed by the factors related with the secured online transaction system such as confidentiality, integrity and encryption. The findings (in the Malaysian context) of this study supports previous theoretical proposition that transaction security and data privacy are the biggest concerns among the consumers for the enhancement of their confidence to adopt e-commerce (Berendt et al., 2005; Sulaiman, 2000).

5 Managerial implications

The present research finds that security and privacy over online transaction process and trust and reliability of online vendors affect consumers' confidence in adopting e-commerce. Therefore, those organisations that are involved in e-commerce are expected to take a note of the findings, especially in the Malaysian context. All possible security measures should be taken while doing business in the internet. Special attention should be paid on how information provided by the customers is collected, handled, communicated to the legitimate users of the organisation and finally, kept in their systems.

The organisations should look for zero fraud in e-commerce transactions. This can be ensured by zero customer complaints. Utmost care should be taken to keep the customers

confidential information in safe custody. To boost trust in the organisation's offering, the enterprise must be providing high quality product, and support services with reasonable price in a shorter delivery time.

6 Limitations of the study

The study did not link demographic information with the research hypotheses. Further, since sampling was based on convenience, there are chances that the responses provided might not be the true reflection of the population in general and the findings may not represent Malaysian consumers as a whole; therefore, any generalisation of the findings may not be 100% reliable. Thus, studies of a similar nature with different types of cultural settings are recommended before trying to generalise the findings. Further, only selected respondents participated in this study and therefore a self-selection bias might have affected the findings of this study and it may also limit the generalisibility of the findings. Extensions of this study in other settings and using other data collection methods may provide additional insights in the findings. Finally, it is to be noted that this study was based on consumers' perception on perceived security and privacy to adopt e-commerce instead of investigating the effects of perceived security and privacy on actual buying behaviour of the online consumers in future.

As an avenue for further research, we suggest to investigate how commercial websites are designed to be secure, how well these sites recognise the issue of privacy and how well these sites meet consumer needs.

7 Conclusions

About 82.9% of the participants indicated that when online vendors provide all necessary guarantees to ensure security and privacy of personal data, their confidence to adopt e-commerce would increase. The message here is simple and clear that in order that a web-based business to survive and strive, it has to assure its customers that their personal information is protected. In addition, this empirical study further concludes that the lack of trust and reliability of online vendors are stopping large number of consumers from engaging in commercial web transactions. This is evidenced by the fact that approximately 80% of the respondents indicated that they do not simply trust online vendors to engage in transactions involving money and personal information. As trust lies at the heart of enduring B2C e-commerce relationship, our findings suggest that online vendors need to find ways of improving consumers' perception of their trustworthiness and reliability in order to exploit fully the potential of e-commerce for the benefit of consumers and merchants alike.

The overall findings show that the model used for testing relationships between consumers' confidence to adopt e-commerce and each of the factors discussed has some predictive power and can be used to capitalise on new marketing opportunities afforded by advanced communication technologies. The findings are expected to provide guidelines to the marketers who are looking for ways to capitalise on new market opportunities with advanced technologies. In order for e-commerce to be accepted and spread in the society, consumers must be informed about how their concerns on the security of electronic exchanges or privacy issues are addressed particularly with the

development of internet payment systems. Furthermore, e-commerce education and awareness programs among internet users would enhance the growth and adoption of online commercial activities.

References

Ahuja, M., Gupta, B. and Raman, P. (2003) 'An empirical investigation of online consumer purchasing behaviour', *Communications of the ACM*, Vol. 46, No. 12, pp.145–151.

Azmi, I.M. (2002) 'E-commerce and privacy issues: an analysis of the personal data protection bill', *International Review of Law Computers and Technology*, Vol. 16, No. 3, pp.317–330.

Basu, A. and Muylle, S. (2003) 'Authentication in e-commerce', *Communications of the ACM*, Vol. 46, No. 12, pp.159–166.

Berendt, B., Günther, O. and Spiekermann, S. (2005) 'Privacy in e-commerce: stated preferences vs. actual behaviour', *Communications of the ACM*, Vol. 48, No. 4, pp.101–106.

Bingi, P., Mir, A. and Khamalah, J. (2000) 'The challenges facing global e-commerce', *Information System Management*, Vol. 17, No. 4, pp.26–34.

Blount, Y., Castleman, T. and Swatman, P.M.C. (2005) 'E-commerce, human resource strategies, and competitive advantage: two Australian banking case studies', *International Journal of Electronic Commerce*, Vol. 9, No. 3, pp.73–89.

Braithwaite, T. (2002) *Securing E-Business Systems- a Guide for Managers and Executives*, New York: John Wiley & Sons, Inc.

Cheung, C.M.K. and Lee, M.K.O. (2001) 'Trust in internet shopping: instrument development and validation through classical and modern approaches', *Journal of Global Information Management*, Vol. 9, No. 3, pp.23–31.

Ching, H.L. and Ellis, P. (2004) 'Marketing in cyberspace: what factors drive e-commerce adoption?', *Journal of Marketing Management*, Vol. 20, pp.409–429.

Economist Intelligence Unit (2006) 'Overview of e-commerce in Malaysia', *The Economist*, 13 June, Available at: http://globaltechforum.eiu.com/index.asp?layout=printer_friendly&doc_id =8706.

Fraser, S. and Wresch, W. (2005) 'National competitive advantage in e-commerce efforts: a report from five Caribbean nations', *Perspectives on Global Development and Technology*, Vol. 4, No. 1, pp.27–44.

Ghosh, A.K. (2001) *E-commerce Security and Privacy*, Berlin: Kluwer Academic Publishers.

Grandon, E. and Pearson, J.M. (2004) 'E-commerce adoption: perceptions of managers/owners of small and medium sized firms in Chile', *Communication of the Association for Information Systems*, Vol. 13, pp.81–102.

Head, M.M. and Hassanein, K. (2002) 'Trust in e-commerce: evaluating the impact of third-party seals', *Quarterly Journal of Electronic Commerce*, Vol. 3, No. 3, pp.307–325.

Heuvelmans, P. (2000) 'The effect of security measures on consumer's behaviour', Available at: http://www.paul3.demon.co.uk/papers/ecom_security.html. Accessed on October 2005.

Hynes, N., Gurau, C. and Chan, H.W.K. (2006) 'Consumer trust and its effect on sustainable e-commerce development in China', *Entrepreneurship, Management and Sustainable Development*, Vol. 2, Nos. 1/2, pp.23–35.

Javalgi, R.G., Wickramasinghe, N., Scherer, R.F. and Sharma, S.K. (2005) 'An assessment and strategic guidelines for developing e-commerce in the Asia-Pacific region', *International Journal of Management*, Vol. 22, No. 4, pp.523–531.

Jawahitha, S. (2004) 'Consumer protection in e-commerce: analyzing the statutes in Malaysia', *The Journal of American Academy of Business*, Vol. 4, Nos. 1/2, pp.55–63.

Khatibi, A., Thyagarajan, V. and Seetharaman, A. (2003) 'E-commerce in Malaysia: perceived benefits and barriers', *Vikalpa*, Vol. 28, No. 3, pp.77–82.

Koch, M. and Möslein, K.M. (2005) 'Identities management for e-commerce and collaboration applications', *International Journal of Electronic Commerce*, Vol. 9, No. 3, pp.11–29.

Krishnan, G. (2006) 'Internet marketing exposure in Malaysia', Available at: http://www.gobalakrishnan.com/2006/12/malaysia-internet-marketing/.

Looi, H.C. (2005) 'E-commerce adoption in Brunei Darussalam: a quantitative analysis of factors influencing its adoption', *Communication of the Association for Information Systems*, Vol. 15, pp.61–81.

Molla, A. and Licker, P.S. (2005) 'Perceived e-readiness factors in e-commerce adoption: an empirical investigation in a developing country', *International Journal of Electronic Commerce*, Vol. 10, No. 1, pp.83–110.

Paynter, J. and Lim, J. (2001) 'Drivers and impediments to e-commerce in Malaysia', *Malaysian Journal of Library and Information Science*, Vol. 6, No. 2, pp.1–19.

Porter, M.E. (2001) 'Strategy and the internet', *Harvard Business Review*, Vol. 79, No. 3, pp.62–79.

Ratnasingam, P. and Phan, D.D. (2003) 'Trading partner trust in B2B e-commerce: a case study', *Information System Management*, Vol. 20, No. 3, pp.39–50.

Salam, A.F., Iyer, L., Palvia, P. and Singh, R. (2005) 'Trust in e-commerce', *Communications of the ACM*, Vol. 48, No. 2, pp.73–77.

Salam, A.F., Rao, H.R. and Pegels, C.C. (2003) 'Consumer-perceived risk in e-commerce transactions', *Communications of the ACM*, Vol. 46, No. 12, pp.325–331.

Sharifah, K. (2003) 'Overcoming challenges in telecommunications', *Computimes*, p.10.

Sipior, J.C., Ward, B.T. and Rongione, N.M. (2004) 'Ethics of collecting and using consumer internet data', *Information Systems Management*, Vol. 21, No. 1, pp.58–66.

Sorbel, J. (2003) 'Identity theft and e-commerce web security: a primer for small to medium sized businesses', *SANS Institute*, pp.1–10.

Sulaiman, A. (2000) 'The status of e-commerce applications in Malaysia', *Information Technology for Development*, Vol. 9, pp.153–161.

Turban, E. and King, D. (2003) *Introduction to E-Commerce*, Upper Saddle River, New Jersey: Prentice-Hall, Inc.