STATUS OF THESIS

Title of thesis | THE INVESTIGATION OF THE FACTORS ASSOCIATING CONSUMERS' TRUST IN E-COMMERCE ADOPTION

I, YI YI THAW

hereby allow my thesis to be placed at the Information Resource Center (IRC) of University Teknologi PETRONAS (UTP) with the following conditions:

1. The thesis becomes the property of UTP
2. The IRC of UTP may make copies of the thesis for academic purposes only.
3. This thesis is classified as

☐ Confidential

☑ Non-confidential

If this thesis is confidential, please state the reason:

_____
_____
_____

The content of the thesis will remain confidential for_____ years.

Remarks on disclosure:

_____
_____
_____

Endorsed by

_____ _____

Signature of Author | Signature of Supervisor

Permanent address: No. 17, Court Rd.
Rakhine Packsike Quarter
Kyauk Phyu Township
Rakhine State, MYANMAR

Assoc. Prof. Dr. Ahmad Kamil Mahmood

Date: _____ Date: _____

UNIVERSITI TEKNOLOGI PETRONAS

THE INVESTIGATION OF THE FACTORS ASSOCIATING CONSUMERS' TRUST IN E-COMMERCE ADOPTION

by

YI YI THAW

The undersigned certify that they have read, and recommend to the Postgraduate Studies Programme for acceptance this thesis for the fulfilment of the requirements for the degree stated.

Signature: _____

Main Supervisor: Assoc. Prof. Dr. Ahmad Kamil Mahmood

Signature: _____

Co-Supervisor: Assoc. Prof. Dr. Dhanapal Durai Dominic

Signature: _____

Head of Department: Dr. Mohd Fadzil Bin Hassan

Date: _____

# THE INVESTIGATION OF THE FACTORS ASSOCIATING CONSUMERS' TRUST IN E-COMMERCE ADOPTION

By

YI YI THAW

A Thesis

Submitted to the Postgraduate Studies Programme

as a Requirement for the Degree of

DOCTOR OF PHILOSOPHY

DEPARTMENT OF COMPUTER AND INFORMATION SCIENCES

UNIVERSITI TEKNOLOGI PETRONAS

BANDAR SERI ISKANDAR,

PERAK

JUNE 2011

DECLARATION OF THESIS

Title of thesis | THE INVESTIGATION OF THE FACTORS ASSOCIATING CONSUMERS' TRUST IN E-COMMERCE ADOPTION

I, YI YI THAW

hereby declare that the thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UTP or other institutions.

Witnessed by

| | |
|---|---|
| Signature of Author | Signature of Supervisor |
| Permanent address: No. 17, Court Rd.<br>Rakhine Packsike Quarter<br>Kyauk Phyu Township<br>Rakhine State, MYANMAR | Assoc. Prof. Dr. Ahmad Kamil Mahmood |
| Date: _____ | Date: _____ |

ACKNOWLEDGEMENTS

First and foremost, all praises and thanks are due to Allah(*Subhanahu Wa Taala*) for giving me the strength, patience, courage and determination in compiling this work, and may peace and prayers be upon our Prophet Muhammad(*Salla Allahu alayhi Wasalam*).

I wish to express my sincere gratitude to my supervisors, Associate Professor Dr. Ahmad Kamil Mahmood and Associate Professor Dr. Dhanapal Durai Dominic, for their invaluable guidance, instructions, encouragement and full support that led my research work to success.

This academic process paralleled the growth and maturation of my little daughter, Arifa, from baby to young little girl. Arifa has been the one most inspiring factor all the way through this academic endeavor. By looking into her curious eyes would never let me tire on the path toward accomplishing this doctoral degree. Most of all, special thanks to my beloved husband, Imran, for being there for me.

My special gratitude goes to my parents, for their love, patience and faith throughout my doctoral study. I am thankful to my brother and sisters for all their support.

I would like to thank all the respondents who used some of their valuable time to complete the survey questionnaires. I am also grateful to all of my friends for their ideas, encouragement and concerns during the difficult time of my doctoral study. May Allah(*Subhanahu Wa Taala*) always bless you all, Ameen!

ABSTRACT

The success of electronic commerce significantly depends on providing security and privacy for its consumers' sensitive personal information. Consumers' lack of acceptance in electronic commerce adoption today is not merely due to the concerns on security and privacy of their personal information, but also lack of trust and reliability of web vendors. Consumers' trust in online transactions is crucial for the continuous growth and development of electronic commerce. Since Business to Consumer (B2C) e-commerce requires the consumers to engage the technologies, the consumers face a variety of security risks. This study addressed the role of security, privacy and risk perceptions of consumers to shop online in order to establish a consensus among them. The findings provided reliability, factors analysis for the research variables and for each of the study's research constructs, correlations as well as regression analyses for both non-online purchasers' and online purchasers' perspectives, and structural equation modeling (SEM) for overall model fit. The overall model was tested by AMOS 18.0 and the hypothesis, assumptions for SEM and descriptive statistics were analyzed by SPSS 12.0.

The empirical results of the first study indicated that there were poor correlations existed between consumers' perceived security and consumers' trust as well as between consumers' perceived privacy and consumers' trust regarding e-commerce transactions. However, the construct of perceived privacy manifested itself primarily through perceived security and trustworthiness of web vendors. While trustworthiness of web vendors was a critical factor in explaining consumers' trust to adopt e-commerce, it was important to pay attention to the consumers' risk concerns on e-commerce transactions. It was found that economic incentives and institutional trust had no impact on consumers' perceived risk.

Findings from the second study indicated that perceived privacy was still to be the slight concern for consumers' trust in e-commerce transactions, though poor

relationships or associations existed between perceived security and consumers' trust, between trustworthiness of web vendors and consumers' trust, and between perceived risk and consumers' trust. The findings also showed that the construct of perceived privacy manifested itself primarily through perceived security and trustworthiness of web vendors. It was found that though economic incentives influenced a consumers' perceived risk in online transactions, institutional trust had no impact on consumers' perceived risk.

Overall findings suggested that consumers' perceived risk influenced their trust in e-commerce transactions, while the construct of perceived privacy manifested itself primarily through perceived security as well as trustworthiness of web vendors. In addition, though economic incentives had no impact on consumers' perceived risk, institutional trust influenced a consumers' perceived risk in online transactions. The findings also suggested that economic incentives and institutional trust had relationships or associations with consumers' perceived privacy.

The findings from this research showed that consumers' perceived security and perceived privacy were not mainly concerned to their trust in e-commerce transactions though consumers' perceived security and perceived privacy might slightly influence on the trustworthiness of web vendors in dealing with online store sites abroad. Furthermore, consumers' perceptions on the trustworthiness of web vendors were also related to their perceived risks and the concern about privacy was also addressed to perceived risks.

Index terms: Perceived security; perceived privacy; perceived risk; trust; consumers' behaviour; SEM

# ABSTRAK

Keberkesanan elektronik dagang (e-dagang) berkait rapatdengan jaminan keselamatan dan privasi terhadap maklumat peribadi pengguna yang sensitif. Namun, bukan itu sahaja factor penyebab kurangnya kepercayaan para pengguna terhadap e-dagang, ia termasuk jaminan daripada pihak yang menyediakan laman sesawang tersebut. Kepercayaan para pengguna terhadap transaksi atas talian sangat penting agar e-dagang dapat terus berkembang. Konsep Perniagaan Kepada Pengguna (B2C) di dalam e-dagang melibatkan penggunaan berbagai teknologi di mana para pengguna teknologi tersebut terdedah kepada pelbagai risiko keselamatan. Kajian ini mengetengahkan peranan keselamatan, privasi dan tanggapan terhadap risiko oleh pengguna dalam urus niaga di atas talian agar semua isu yang disebut dapat diperjelaskan. Kajian ini mengetengahkan kepercayaan, faktor analisis untuk pembolehubah kajian ini dan pembinaan kajian, hubungkait dan analisis regrasi perspektif untuk situasi bukan pembeli atas talian dan pembeli atas talian serta struktur persamaan permodelan (SEM) untuk keseluruhan model. Keseluruhan model diuji menggunakan AMOS 18.0 manakala hipotesis, jangkaan SEM dan gambaran statistic dianalisis oleh SPSS 12.0.

Hasil kajian situasi yang pertama mendapati hubung kait yang lemah di antara tanggapan keselamatan dengan kepercayaan oleh pengguna dan juga di antara tanggapan privasi dengan kepercayaan pengguna terhadap transaksi e-dagang. Walaubagaimanapun, tanggapan privasi dilihat sebagai aspek utama melalui tanggapan keselamatan dengan kebolehpercayaan terhadap pihak yang menyediakan laman sesawang. Sehubungan dengan itu, perhatian yang lebih juga patut diberikan kepada tanggapan risiko-risiko oleh pengguna terhdap e-dagang. Kami mendapati insentif ekonomi dan kepercayaan sesuatu institusi tidak mempengaruhi tanggapan risiko para pengguna.

Hasil daripada kajian situasi kedua memperlihatkan tanggapan privasi oleh pengguna masih rendah dalam kepercayaan pengguna transaksi e-dagang, malahan hubungkaitan yang lemah di antara tanggapan keselamatan dengan kepercayaan oleh pengguna, di antara kebolehpercayaan kepada pihak penyedia laman sesawang dengan kepercayaan pengguna, dan juga di antara tanggapan risiko dengan keprcayaan pengguna. Kajian ini juga menunjukkan tanggapan privasi dilihat sebagai aspek utama melalui tanggapan keselamatan dengan kebolehpercayaan pada penyedia laman sesawang. Kami juga mendapati insentif ekonomi mempengaruhi tanggapan risiko pengguna terhadap transaksi atas talian, namun sebaliknya dalam konteks tanggapan risiko oleh pengguna.

Secara keseluruhannya, tanggapan risiko pengguna memperngaruhi kepercayaan mereka dalam transaksi e-dagang, sementara tanggapan privasi pengguna dilihat sebagai aspek utama melalui tanggapan keselamatan, serta kebolehpercayaan pada penyedia laman sesawang. Tambahan lagi, insentif ekonomi tidak mempengaruhi tanggapan risiko pengguna pada transaksi atas talian. Hasil kajian turut menyetakan bahawa insentif ekonomi dan kepercayaan institusi mempunyai hubungkait dengan tanggapan privasi pengguna.

Kesimpulan daripada kajian ini menunjukkan bahawa tanggapan keselamatan pengguna dengan tanggapan privasi tidak member impak yang besar dalam mempengaruhi kepercayaan pengguna dalam melakukan transaksi e-dagang; walaupun tanggapan tersebut mungkin memberi impak yang agak sederhana terhadap penyedian laman sesawang dalam transaksi atas talian antarabangsa. Tambahan pula, tanggapan pengguna terhadap kebolehpercayaan pada penyedia laman sesawang mempunyai hubungkait dengan tanggapan risiko dan mengambil berat tentang privasi juga diketengahkan oleh tanggapan risiko.

Indeks: Tanggapan keselamatan; tanggapan privasi; tanggapan risiko; kepercayaan; tingkahlaku pengguna; SEM

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

# CHAPTER 1

# INTRODUCTION

## 1.1 Introduction

The Internet has brought its place as a vital part of our lives. In this Internet age, one of the most essential areas which is considerably transformed by the Internet and World Wide Web is the way people around the world purchasing and selling products and services in the online competitive environment, that is, Electronic Commerce. The utilization of the Internet with rapid advances in technology has become a tool that allows people around the world to chat and do business efficiently and powerfully. E-commerce has different definitions depending on whom we ask. Turban et al. (2009) defines Electronic commerce (EC) as the procedure of purchasing, selling, transferring or exchanging products, services, and / or information via communication networks, including the Internet. In this study, e-commerce is broadly defined as the exchange relationship between consumers and web vendors over the Internet.

The terms, e-commerce and e-business are often used exchangeable. In practice, e-business not only consists of the selling of products and services, but also serving consumers and cooperating with business collaborators. For example, as a part of e-business, all means of communication such as, email, and chat rooms are used to provide services to customers and talk to business associates an online store. Therefore, e-commerce is a sub-set of an entire e-business strategy while e-business focuses on more strategic manner by emphasizing on the functions that happen using electronic means. E-business makes use of information technology applications and infrastructure to optimize and create existing and new business process (Alan, 2000).

To enhance the efficiency of the system by using technology transforms traditional commerce into electronic commerce. We are living in advance interesting time now, with apparently limitless improvements and evolution in the high technology sector. Electronic commerce has stepped up worldwide market and, thus, has had an enormous outcome on the overall economy (Hwang et al., 2006). Hence, there is a need to continue for furthering education and reassessment of the computing systems, security mechanisms as well as business models used by online companies.

Our access to products and services are greater than people could ever have imagined previously. The growing popularity of electronic commerce offers more opportunities for businesses and consumers. With the advancement of information technologies, we can do many things in 24 hours a day from thousands of miles away. Hence, electronic commerce has basically transformed the way business is done by the organisations and the way products and services are bought and sold by the consumers. Internet based e-commerce represents an enormous opportunity for cost reduction and process streamlining. Many public and private sectors, such as e-learning, monetary services, and information retrieval, are utilizing the services available through electronic commerce by including ideas of suitable and personalized services, such as marketing, advertising, and personalized learning for consumers. Moreover, Dinev and Hart (2006) stated that the services, such as online tax registering and electronic voting are offered by the governments in many well-developed and developing countries to the general public on the Internet.

Though the Internet makes our lives easier, it also opens the doors to the criminal activities on our personal information, our security and safety. The effects of viruses, hackers, crackers and worms can make complete disasters. Thus protection of digital identity is very essential. In general, it is cheaper to take preventative measures than respond to disasters in loss of information or control in dealing with digital world. For e-commerce to become mainstream, we still face with one obstacle. Users of these technologies need to become comfortable in understanding and applying the new business risk models that bring the new technologies to bear. As the Internet has developed in complexity and ambiguity, many consumers feel the web vendors may be gathering and sharing their sensitive personal information without their consent or

knowledge. Therefore, we need adequate control on our sensitive personal information we provide to online store sites.

For those looking for the advantages of electronic commerce, the Internet provides huge benefits. Unhappily, major significant deficiency of the e-commerce, compared to traditional commerce, is totally public. Without the use of specialized security technologies and supporting infrastructure, transaction contents can be read by, modified by, or trumped up by anyone who is sufficiently obstinate. Failure to meet the security challenge would severely undermine the commercial exploitation potential of the Internet, owing to low user confidence, and high costs of repeatedly reacting and controlling to security attacks.

In general, it is recognized that adequate security and privacy assessments are extensively required for e-commerce, and indeed e-business applications of all manner, running on the World Wide Web. According to Braithwaite (2002), the security of e-business could be simply explained as how the information is gathered and shared, how the systems process and correspond that information, the confidentially of information, and how the system resources are assembled and prepared securely to make sure its accessibility to rightful parties and consumers. Therefore, security is a continuous process, which is ongoing within organization and it is not a product to be purchased. In order to reduce risks and threats to the company, daily implementation of the system must be done.

Many consumers feel displeased for providing their sensitive personal information, when they engage in online business transactions though they value the advantages of the use of e-commerce. According to Dinev and Hart (2006), many consumers are worried about their liabilities related to privacy of sensitive personal information. In order to realize or sustain the visions of the use of Internet, public and private organizations need to gather consumers' sensitive personal information. Certainly, consumer information has turned out to be one of most desired assets for the growth and development of e-commerce.

It is clear that there is conflict between two trends in e-commerce. Web vendors need to gather consumers' personal information to provide them with better services. On the other hand, the consumers' increasing concern for the exposure and risk to

their sensitive personal information shape an incompatible tendency in e-commerce. Therefore, It is essential to resolve this conflict because it will assist in the better utilization of e-commerce and, thus, in the growth of overall economy. Despite the fact that electronic commerce has turned into an essential matter with the growth and development of Internet in many countries, it is essential to handle the consumers' concerns on security and privacy issues, trustworthiness of web vendors as well as consumers' risk perception. This study, therefore, attempts to recognize the influencing factors for the accepting of possible ways for justifying consumers' concerns in order to participate in e-commerce transactions and, thereby, aiding the growth and developments of e-commerce.

### 1.2 Statement of the Problem

The growth of web based electronic commerce across the world in the past few years offers an opportunity for business firms to expand their presence in the competitive online environments beyond different geographical borders and has generated considerable diversity and complexity in its structure and applications. The potential for the web vendors to succeed in these global online environments depends on the presences of consumers on the World Wide Web and the pace at which consumers will change to electronic transaction (Hoffman and Novak, 1999). Electronic commerce embraces vast prospective for transforming the businesses and economy globally. Thus, the utilisation of e-commerce and the revenues to understand its full prospective are of vital significance for the enlargement of the overall economy (Javalgi et. al., 2005). However, e-commerce, at present, embraces a little contribution of the overall economy. According to Brown and Riley-Katz (2008), nowadays, Amazon, eBay, and Yahoo Shopping become the main e-commerce businesses players, and thus, substantial contributors of their country's economy.

In today's economy, one of the most important challenges in dealing with e-commerce transactions is the apparent lack of sufficient security to secure consumers' financial and sensitive personal information, and web technologies on which people rely. Attacks on the nation's information processing infrastructure are becoming an

increasing serious problem in today's online economy. The increase in the growth of incidents is reflecting the growth of the Internet, and the intended increase in e-commerce can only make worse this upward trend.

Electronic commerce has observed a period of rapid growth in a commercially self-regulated online environment. However, despite the fact that e-commerce is disseminating globally, lots of consumers are still hesitant to engage in it due to the security and privacy issues (Hoffman et al., 1999; Bingi et al., 2000; Godwin, 2001; Belanger et al., 2002; Basu and Muylie, 2003; Ahuja et al., 2003; Mustafa and Mohd Khairuddin, 2003; Yusof and Mohd Yusof, 2005 and Ahmed et al.,. 2007). Singh and Hill (2003) stated that with advent information technology, information privacy issue has become increasingly important, and as consumer supporters, web vendors face difficulties to find potential means to care for their consumers' privacy.

According to Grupe et al. (2002) and Milberg et al. (2000), many developed countries have applied various methods in order to response to public concerns on privacy in dealing with e-commerce. For example, the USA has mainly trusted on online businesses to control their consumers' sensitive personal information freely, while EU member countries already have carried out certain degree on controlling consumers' sensitive personal information (Faja et al., 2006). However, Ashrafi (2005) and McKenna (2001) stated that while some individuals consider this to be a further business responsive, other individuals consider it a lack of hardness. Competitive online business environment is forcing businesses to gather consumers' sensitive personal information more and more, with the purpose of knowing consumers' desires and needs. With the advent information technology, it is possible to quickly gather, analyse and transfer huge amounts of consumers' sensitive personal information. Therefore, consumers' security and privacy are violated due to the enlarged gathering and using of consumers' sensitive personal information. Web vendors attempt to achieve their consumers' trust by using the trusted web seals on their store sites. Trusted third parties approve web seals to confirm that the online store site has met certain standards for security and privacy policies.

The researches have exposed that consumers' perceptions on privacy breach and risk could be manipulated by actions of web vendors. Many web vendors have taken

some of the actions to ease their consumers' privacy and risk concerns. For examples, offering economic incentives, such as providing lower price and higher quality can reduce consumers' perceived risk (Salam et al., 2003), and offering financial incentives, such as offering discounts and prizes, and free shipping were effective in exchange for their consumers' sensitive personal information (Hann et al., 2007). However, some studies that did examine the connection among providing incentives and voluntarily disclosure of consumers' personal information found conflicting outcomes. That is, though findings from Hann et al. (2007) revealed that online store sites that provided incentives, such as a financial incentive and potential easiness considerably improved consumers' favourites for those online store sites, a study by Ward et al. (2005) investigated that incentive rewards, such as financial discount and customized service were not significantly affected in order to gain consumers' sensitive personal information.

With the revolution of World Wide Web, the issue of privacy has become more sensitive with vital implications for the online marketspace. The Internet could be used to gather consumers' sensitive personal information, and then those collected information could be utilized by web vendors for their own gains. Indeed, consumers' privacy concern has been recognized as the major obstacle in dealing with e-commerce transactions (Graeff and Harmon, 2002) and this is one of the significant barriers to e-commerce growth and development. Particularly, Dinev and Hart (2006) stated that consumers have acknowledged the necessity to disclose their sensitive personal information as the major issue that stopped them from engaging in e-commerce transaction. Media exposure on security and privacy issues also serve to boost consumers' security and privacy concerns to trust in e-commerce transactions involving financial and sensitive personal information.

Poindexter et al. (2006) expected that consumers' security and privacy concerns related to their sensitive personal information will probably rise for few more years. Protecting the consumers' privacy has become very important in both the public and private organizations due to the illegal performances of information stealing over the Internet (Brannen, 2007). Therefore, consumers are so worried regarding the security and privacy of their financial and other sensitive personal information in order to deal with online businesses over the Internet and World Wide Web. Malhotra et al. (2004)

stated that consumers' privacy concern is observed as a main threat to e-commerce. In most of the privacy literatures, security and privacy concerns are treated as a single construct (Liu et al., 2004 and Belanger et al., 2002). According to Liu et al. (2004), caring privacy of consumers' sensitive personal information is a significant aspect for the growth and development of e-commerce. In reality, consumers are hesitant to transact online since they need to reveal their sensitive personal information such as credit card information, contact number and so on. However, it is necessary for web vendors to gather consumers' information, with the intention to achieve a better understanding of consumers' activities and favorite choices. Hence, a difficult responsibility which web vendors face is in gathering necessary consumers' personal information required, without compromising consumers' privacy, to build up policies for consumers' detention and market enlargement.

Considerable numbers of researchers (Ahmed et al.,. 2007; Salam et al., 2003 and Basu and Muylie, 2003) have indicated that consumers' acceptance of e-commerce transaction is rising slowly for the reason that they merely do not trust most online store sites today to transact in exchange relationships requiring financial and sensitive personal information. Web vendors use the advent of technological capabilities such as client-server systems and Enterprise Resource Planning (ERP) to collect, store and exchange consumers' personal information to develop strategies for market growth. Sometimes, without consumers' permission, web vendors collect information about their consumers' behavior and preferences to trace their consumers' actions on the Internet (Olivero and Lunt 2004). The potential risk related to the misuse of consumers' sensitive personal information gathered by web vendors, such as, sharing information with unauthorized third parties has also been highlighted.

The consumers' concerns about security and privacy in dealing with e-commerce transactions have become major reason for the slowly growth of e-commerce. In reality, consumers need to give much sensitive personal information to web vendors in order to deal with e-commerce transactions (Feigenbaum et. al., 2009). As a result of this, the consumers' concern for information security and privacy has been increasing in order to transact with web vendors. Primarily, consumers' increased concerns on security and privacy lead to the lack of trust on web vendors, and, consequently, reluctant to engage in e-commerce transactions (Miyazaki, 2008).

Web vendors have already tried to resolve consumers' concerns on security, privacy, trust and risk by providing economic and financial incentives and to gain their consumers' sensitive personal information. A study by Salam et al. (2003) reported that consumers' perceived risk in e-commerce transactions is reduced with the increase in economic incentives and institutional trust. Though consumers' names and e-mail addresses can be given easily to web vendors for a financial and economic incentives, other sensitive information, such as, their credit card numbers, will not be easily given to web vendors for the purpose of getting monetary benefits and discounts.

Web vendors use some of the illegal information gathering practices for their consumers that lead to consumers' privacy concerns. To mitigate these kinds of consumers' privacy concerns, trustworthiness and reliability of web vendors has been recognized as a significant determinant of consumer behavior in dealing with e-commerce transactions (Liu et al., 2004; Malhotra et al., 2004 and Luo, 2002). According to Gefen et al. (2003), consumers expect trustworthiness and reliability of web vendors in engaging in e-commerce transactions involving financial and sensitive personal information.

Trust can also be viewed as a vital factor to lessen consumers' perceived risk and uncertainty to engage in e-commerce transactions. When consumers are dealing with online businesses, they perceive significant risks and uncertainty because of some essential factors, such as security and privacy of their sensitive personal information, uncertainty about web vendors' characteristics and performances, incapability to check the products, incapability to observe the acts of the online store sites, and so on. McKnight et al. (2002b) stated that trust in online store sites enhances the possibility that the consumers will be willingly to deal with e-commerce transactions. This means that the consumers' perceived risk originating from their concerns on security and privacy decline to some extent by trusting online store sites. Some consumers will calculate the possible risk, that can be featured to some amount to their security and privacy concerns of their sensitive personal information and the benefits of engaging in online business transactions, then will reach the decisions as whether to engage in e-commerce transactions.

Regardless of e-commerce offers many chances and guarantees to the consumers, the figure of consumers engaging in e-commerce transactions are in small numbers compared to the figure of consumers accessing the web for other purposes. Even though web based electronic commerce has been spread around the world with significant speediness, there are still major variations in the trust and acceptance of the Internet for commercial purposes among consumers across the world because of trust, privacy and security concerns. Many consumers are wondering whether electronic form of commerce is as secure as traditional business conduct.

In dealing with e-commerce nowadays, both consumers and web vendors face high level of uncertainties because it is not possible to authenticate the involved parties physically over the Internet. Since e-commerce is a form of commerce using technology and it is conducted through computer networks, concerns about security, privacy, authentication, trust, risk of loss and fraud are frequently cited among the major barriers to the development and growth of e-commerce.

Threats to e-commerce are regularly altering and thus, the technologies of countermeasure must transform in reaction. Solutions for the security problems of today will not be sufficient next year as e-commerce architectures evolve and new business applications are embraced. Therefore, nowadays, the issues on security, privacy, trustworthiness of web vendors and risks are of more concerns than always before whilst the emerging information technologies are considerably changing the ways businesses are carried on. In summary, the problem statements are as follows:

- Despite the fact that e-commerce is disseminating globally, lots of consumers are still hesitant to engage in it due to the security and privacy issues.
- Consumers' acceptance of e-commerce transaction is rising slowly for the reason that they merely do not trust most online store sites today to transact in exchange relationships requiring financial and sensitive personal information.
- When consumers dealing with online businesses, they perceive significant risks and uncertainty.

## 1.3 Research Motivations

Researches in consumer behaviour, security, privacy, trust, risk and e-commerce have examined the relationship of security, privacy, trust and risk with behaviour in separate studies. Consumer behaviour and security have been well studied in e-commerce researches (Carlos and Miguel, 2006; Laforet and Li, 2005; Kai et al., 2004; Suh and Han, 2003; Yang and Jun, 2002 and Salisbury et al., 2001). Researchers have also well studied consumer behaviour and privacy (Babita et al., 2010; Lanier and Saini, 2008 and Stewart and Segars, 2002). Consumer behaviour and trust have also been researched (Pavlou, 2003; McKnight et al., 2002b and Jarvenpaa et al., 2000). Researchers have also studied consumer behavior and risk (Doney at al., 2007; Pavlou and Gefen, 2004 and Salam et al., 2003).

The adoption of electronic commerce significantly requires a consumer to make decisions in an environment of critical opposing forces, namely, security and privacy concerns, trust, and risk perception. For that reason, it is essential to study the adoption of e-commerce in a holistic way by taking into consideration of the impact of these associated significant factors. To author's knowledge, this is the initial research to investigate these factors together in a single study regarding Malaysian consumers' trust in e-commerce adoption. The main motivations of this study are: to provide a clear description of security and privacy concerns; to provide an integrative framework for the adoption of ecommerce by adapting security and privacy concerns, trustworthiness of web vendors and risk perceptions; and empirically validate the proposed research framework.

### 1.3.1 Research Questions

a) Do consumers' security and privacy concerns of online transaction significantly relate to their trust in e-commerce adoption?
b) How do the trustworthiness of the web vendors relate to the consumers' adoption of e-commerce?
c) How do economic incentives and institutional trust relate to consumers' perceived risk in order to adopt e-commerce?

d) What are the inter-relationships of security, privacy, trustworthiness of web vendors and risk perceptions, and how do these factors affect consumers' behaviour intention to adopt e-commerce?

## 1.4 Objectives of the Study

The Internet together with emerging information technologies has particularly enlarged public concerns intended for information security and privacy. Information security, privacy and risk are becoming the primary concerns of today's e-commerce environment, which utilize the Internet for commercial purposes as well as keeping relationships with business partners. However, in today's e-commerce environment, the participation of all parties needs to involve by working together in order to achieve secure information successfully.

In addition, this study examines whether trust would assist consumers and web vendors in an equally valuable way and probably lead to more beneficial utilization and development of e-commerce. The development and growth of e-commerce will eventually contribute to the growth of overall country's economy. Studying whether consumers, in reality, concern security, privacy, risk as well as trust beliefs of web vendors could inform web vendors when and what sorts of consumers' information they might be able to reach consumers' trust in e-commerce transactions. Providing consumers' information without compromising their privacy can benefit web vendors through with more beneficial product advertising and in turn, increase in overall sales. The consumers can get advantages through more product selections and better beneficial in product purchasing and utilization of services provided by web vendors.

The main objective of this study is to identify the factors that contribute to the consumers' willingness to engage in e-commerce transactions, and further study the relationship between those factors. Therefore, this study will focus on the following sub-objectives:

a) To study whether or not consumers' perceived security and privacy of online transaction significantly affect their confidence to adopt e-commerce.

b) To identify the factors of trust with web vendors to engage in transactions involving money and sensitive personal information.

c) To study the role of economic incentives and institutional trust related to consumers' perceived risk in order to adopt e-commerce.

d) To study the relationship between security, privacy, trustworthiness of web vendors and risk perceptions in e-commerce adoption.

## 1.5 Significance of the Study

Electronic commerce is rapidly growing business medium, and it has radically altered the marketing and distribution paradigms. Yet, small concerning has been made publicity on the consumers' views in dealing with e-commerce towards obstacles in its growth, mainly those established in South East Asia. In Malaysia, e-commerce industries have not taken off as expected though relatively increasing numbers of consumer are participating in e-commerce business transactions.

The significance of this study inhabits the fact that its findings will give web vendors an idea about that there should be in adequate control of the means to ease their consumers' concerns on security and privacy issues related to dealing with e-commerce transactions, and it will lead to the development of trust. Moreover, consumers' concerns on risks associated with providing their sensitive personal information to web vendors might be reduced by offering economic incentives by online store sites. The findings of this study might be a significant affect on the ways and the policies web vendors will have to consider for e-commerce growth and development. In turn, the growth and development of e-commerce could considerably lead to the enlargement of country's economy.

This study examines whether consumers are still so concerned on security and privacy of their sensitive personal information, trustworthiness of web vendors as well as risk associated with providing their sensitive personal information in order to adopt e-commerce. Previous studies (Hann et al., 2007; Ward et al., 2005 and Malhotra et

al., 2004) explored consumers' security and privacy concerns in diverse perspectives, for example, focusing on whether consumers are so concerned on security and privacy of their sensitive personal information to participate in e-commerce transactions.

In some of the privacy literatures, Liu et al. (2004) and Xu and Teo (2004) stated that security and privacy concerns can be treated as a single construct. However, other researchers agreed that security and privacy concerns should be treated as two different concepts (Chang et al., 2005 and Vijayasarathy, 2004). Belanger et al. (2002) also cited that security and privacy concerns should be considered as distinguishable, and that there is a lack of realising of their relations. This study affords to give a clear description of the impact factors of consumers' security and privacy concerns, and whether consumers' privacy concern is mediated by security concern.

Studies indicated that underlying consumers' privacy concerns inspire them to providing false information or withholding their sensitive personal information, whenever relevant, and when the situations of fully disclosure are present (Culnan and Armstrong, 1999 and Hoffman et al., 1999a). The authors have recommended that consumers' privacy concerns may be dealt with through the use of fair information practice by allowing for consumers with more control over their sensitive personal information and formulating trust (Milne, 2000; Phelps et al., 2000 and Culnan and Armstrong, 1999). According to Olivero and Lunt (2004), though providing control over the use of information by adopting fair information practices may reduce the perceived risk associated with secondary information use, there is lack of evidence that informational control would lead to the development of trust. Fair Information Practices (FIP) is a common term for a set of standards governing the gathering and utilization of sensitive personal information and covering the issues of privacy and accuracy.

Nowadays, business is looping with e-commerce. The Internet together with the emerging information technologies has become powerful mediums for participation in e-commerce environment. The use of the Internet together with emerging information technologies has opened for performing e-commerce transactions without geographical limitations, and therefore causing e-commerce is a significant part of the

overall economy. The major feature of any society depends on the country's economy. With the advancements in information technology and its use have normally prepared living more well-organized. As a result, an enhancement in the economy will instantly develop mutual state of individual, and the entire public. As a result, technology has significantly leaded to the constructive community transform. Growth and development of e-commerce is element of the practical application of advents in information technology for the improvement of today's societies.

This study is helpful in providing the consumers' perspectives of e-commerce in terms of barriers to its full scale adoption. Hence, it is expected that these findings should be taken into consideration for promoting e-commerce, especially for the Malaysian consumers. This study will prove to be valuable among enterprises that are dealing with business-to-consumer online transactions. In addition, this study contributes valuable insights into the current consumers' perceptions of e-commerce for researchers those seeking to explore further consumer behavioural research.

### 1.6 Scope and Nature of the Study

This study focuses on the aspect of electronic commerce that utilizes the Internet and the World Wide Web as the technological infrastructure to communicate, distribute and conduct the information exchange that would consequently lead to the commercial transactions between consumers and web vendors.

The nature of this study involved the respondents' aims and views on theoretical assumptions, and the study did not engage respondents' observations in their actual performance. The respondents are studied concerning whether they would like to participate in e-commerce transactions related to their concerns on security and privacy of sensitive personal information, trustworthiness of web vendors as well as their risk perceptions which came to pass under the suggested hypothetical circumstances. Therefore, the nature of the study is mainly based on quantitative surveys added with semi-structured theme interview for detail supporting of this study.

The independent variables in this study were consumers' perceived information security, perceived information privacy, trustworthiness of web vendors, and consumers' risk perception; while the dependent variable was the consumers' trust in e-commerce transaction. Respondents were chosen using sampling procedure, and their responses were assessed by performing data analysis, and the findings were presented for the results, discussions, conclusions and recommendations for further study.

Businesses of all sizes increasingly rely on the information from surveys to discover how to better satisfy their consumers. Therefore, survey method has been mainly adopted in this study since the objective of the research, the availability of resources, the type of information required and the location of the subjects were the factors that contributed to the choice.

## 1.7 Definition of Terms and Concepts

*Authentication*: The process of establishing confidence in the truth of some claims.

*Consumers' Trust:* The probability with which consumers believe that all about dealing with e-commerce transaction is guaranteed as offline transactions.

*Cryptography:* The scientific information encoding (by scrambling the messages into unreadable form) and information decoding (by unscrambling the messages into readable form).

*Customization*: Customization is doing some modification of an existing website's look and feel as per the consumer requirement.

*E-commerce:* The system of business and technological application that facilitates buying and selling of products and services electronically.

*E-commerce Adoption:* The utilization and acceptance of the Internet together with emerging information technologies for the business transactions between consumers and web vendors.

*Economic incentives:* The offering of products or services online at lower price and better quality than that offered in offline store.

*Information privacy*: Information privacy is intentional or unintentional disclosure or misuse of sensitive personal information.

*Institutional trust:* The creating and fostering of trust between consumers' and web vendors alike to facilitate online transactions by financial institutions, such as banks and credit card companies.

*Internet Age*: The Internet Age is presently on-going and it is categorized by the ability of individuals to transact online freely including various activities that would have been difficult or impossible to do previously over the Internet.

*Perceived Privacy:* The likelihood with which consumers consider that their financial and sensitive personal information will be protected by web vendors as they expected.

*Perceived Risk:* The probability with which consumers believe that they will not face unexpected endings with unwanted consequences.

*Perceived Security:* The likelihood with which consumers consider that their financial and sensitive personal information will not be altered during transit and being stored by unintended parties as they expected.

*Personalization*: Personalization is the process of allowing for related content based on individual users' characteristic or preferences.

*Personal information*: Personal information is any information to identify an individual, such as, name, e-mail address, contact number and so on.

*Privacy Violation*: Privacy violation occurs when an online store site gathers and shares individual user's sensitive personal information without his/her consent or knowledge.

*Right to privacy*: Right to privacy refers to an individual user's right to perform his/her matters without intentional or unintentional disclosure or misuse of sensitive personal information.

*Secure Electronic Transaction (SET):* Protocol for secure payment over the Internet.

*Secure Sockets Layer (SSL):* Protocol for secure online communications between consumers and web vendors.

*Trustworthiness of web vendors:* The probability with which consumers believe that the web vendor has some attribute of trustworthiness based on reputation, trusted web seals and recommendation.

*Web browser*: A graphical user interface that provides the capability to view Web pages on the Internet, such as Internet Explorer, Netscape, and Mozilla.

*Web seal:* A logo that represents web assurance services.

*Web vendors:* Also known as online/web merchants, the persons who own the websites and selling their products and services electronically.

## 1.8 Chapter Summary and Organisation of Thesis

The growth and development of e-commerce can count on gathering, storing, and analyzing consumers' personal information with the intention of offering more beneficial products and services, sales improvement, and being competitive in online marketpace. In consequence of more beneficial product and service choices, consumers enjoy the advantages of easiness through e-commerce. On the other hand, because the advent of technological capabilities, such as client-server systems and Enterprise Resource Planning (ERP) make data collection, storage and exchange consumers' personal information more easier without consumers' consent or knowledge. And for the reason that there has been intentional or unintentional disclosure or misuse of consumers' sensitive personal information, consumers' concerns on the use and misuse of their sensitive personal information have become more and more. Therefore, many researches have proven that consumers are reluctant to trust in e-commerce transactions.

Some online businesses have provided economic incentives to relieve consumers' concerns and attract them to disclose their sensitive personal information willingly to web vendors when dealing with e-commerce transactions. Study has proven that providing institutional trust and economic incentives reduce consumers' risk perception. This study examines whether consumers are still concerned about security and privacy of their sensitive personal information, trustworthiness of web vendors as well as risk associated for providing their sensitive personal information in order to participate in e-commerce transaction. In addition, the present study examines whether providing economic incentives and institutional trust reduce consumers' risk perception, and in turn, it will lead consumers to adopt e-commerce transactions.

This study with the introductory chapter that briefly describes the current scenario of electronic commerce with the statement of the problem and objectives of the study. The essence of this thesis is to present the literature of the previous work done on the subject area.

Chapter two is organized in a simple and straightforward manner, with the introduction of e-commerce transaction, available tools and mechanisms for secure e-commerce. A literature review of the study's constructs, namely, perceived security and privacy of online consumer's personal information, and trustworthiness of web vendors and consumers' perceived risk are explained.

Chapter three includes the detail research framework, the chosen research method used to answer the research questions for this study, a description of the research design, the basis for participant selection, the survey instrument and the means for data collection. It also highlights the necessary statistical analysis to be used to carry out the analysis of data findings.

Chapter four presents a detailed analysis and interpretation of study variables and the hypothesized factors based on the research framework developed in chapter 3.

Chapter five presents the further findings related with interviewees' perspectives on dealings with e-commerce adoption.

Chapter six discusses and briefly summarizes the findings of the study, examines the implications of the research findings for theoretical as well as practical use and provides some recommendations for further research.

# CHAPTER 2

# LITERATURE REVIEW

## 2.1 Introduction

This research required to establish consumers' trust to engage in e-commerce transactions as it relates to their perceptions on security, privacy, risk and trust beliefs of web vendors while shopping over the Internet. This chapter reviews the theoretical work as well as the empirical findings of other researches relevant to the objective of this research. Literatures related to e-commerce concepts and framework, research on adoption of e-commerce and in particular, the possible factors influencing consumers' trust in e-commerce transactions, and available tools and mechanisms for secure e-commerce are reviewed in much detail.

## 2.2 E-Commerce on the World Wide Web

Information technologies (IT) enable organisations to carry out trade in more efficient and completely different manners. With the emerging of information technologies, the Internet has formed enormous transform in the trade environment. Novel channels of distribution and supply are promising, and also new marketplaces and exchanges are being shaped electronically, known as Electronic Commerce. Contemporary information technology (IT), however, has always been a source of chance and ambiguity, of benefit and risk.

The growth of electronic commerce in the past few years has changed the way businesses bought and sold products and services, and has also generated considerable diversity and complexity in its structure and applications. Despite the fact that there is no collectively accepted definition of e-commerce, Braithwaite (2002) thinks that e-commerce holds all features of producing, selling and buying products or services electronically. The fundamental features of e-commerce are that two or more people are engaged electronically where information is the main commodity being communicated about the transactions. The e-commerce environment of the Internet is shown in Figure 2.1.

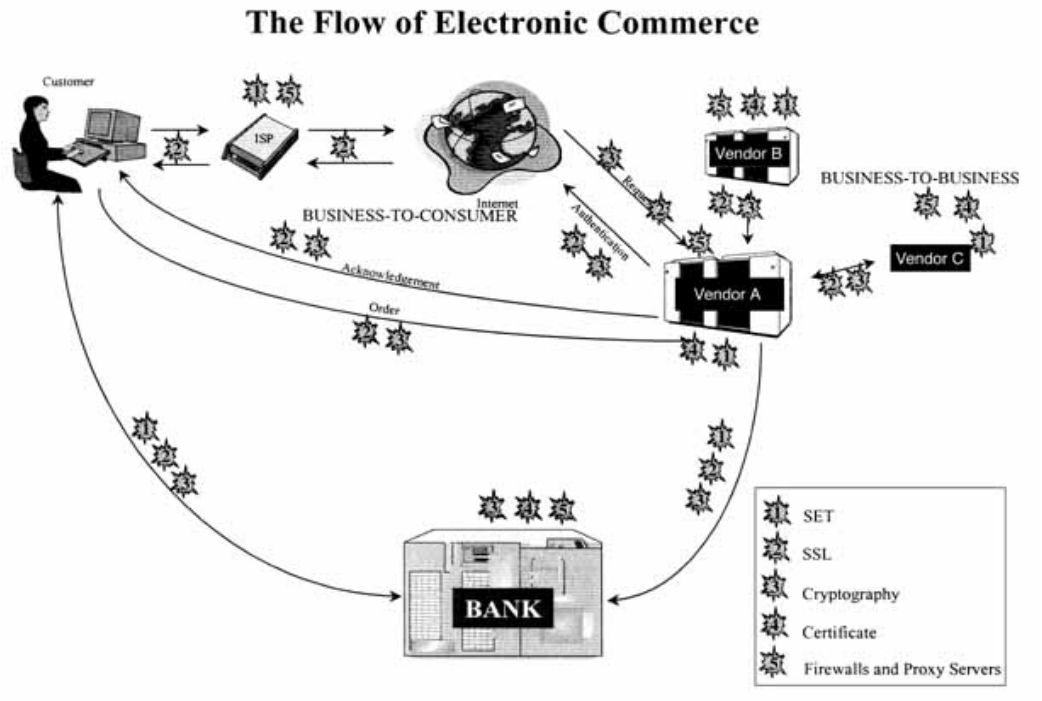



Figure 2.1. The Flow of E-Commerce (Information Systems Audit and Control Foundation, Inc. US).

Many terms, such as e-business, e-government, e-market, and e-trade are used to describe e-commerce. Electronic commerce has different definitions depending on whom we ask.

- From a *communications or technology* perspective, e-commerce is the delivery of information, products, services, or payments via telephone lines, computer networks, or any other means.

- From a *business process or management* perspective, e-commerce is the application of technology toward the automation of business transactions and workflows.

- From a *service or economist* perspective, e-commerce is a tool that addresses the desire of firms, consumers, and management to cut service costs while improving the quality of goods and increasing the speed of service delivery.

- From an *online* perspective, e-commerce provides the capability of buying and selling products and information on the Internet and other online services.

- From a *marketing* perspective, e-commerce is a new medium for providing information to a target market through advertising, promotion, and publicity.

(Kalakota and Whinston, 1997 and O'Daniel, 2000).

All of the definitions from different perspectives can be applied and each of the perspectives may be useful for understanding and implementing an e-commerce business plan. Traditional e-commerce has concerned business-to-business or business-to-government transaction, engaged over closed proprietary systems rather than over the open appearances of the Internet. Today, electronic commerce encompasses nearly any type of commercial transaction. Systems are invented to be business-to-business (B2B), business-to-customer (B2C), business-to-government (B2G), government-to-citizen (G2C) and so on. In any case, the Internet and private communication networks are being used by organizations to set up cooperative strategies with business partners, suppliers, and the consumers.

E-commerce, however, is being attractive in three interconnected dimensions, namely, consumer-to-business dealings, intra-business connections, and business-to-business exchanges. In the consumer-to-business aspect, e-commerce is allowing the consumers to have an ever-increasing say in how products are made, what products are made, and how services are delivered. The up-and-coming forms of the internal

organizational functioning involve transforming in work-group structures, and also in administrative communication, responsibilities, and information flows. In business-to-business dimension, e-commerce makes possible the network form of organization where small enterprises rely on other partner companies for product distribution and component supplies to assemble changing consumer demand more efficiently and effectively.

## 2.3 E-Commerce Security over the Internet

Web technology today allows for numerous criminal activities though it enables incredible marketing, communication, and sales opportunities, that is, e-commerce. Advents in information technology are enabling many new opportunities for security breaches. The Internet, especially the service known as the World-Wide Web, has become the communication interface to an exponentially growing network of computers. The Internet is a massive utility structure for information, communication and media services. Therefore, for e-commerce, Internet offers an easily accessible interface for both buyers and sellers on a global scale. E-commerce is a development by using the Internet as commercial platform. However, the Internet is insecure for many reasons (See Figure 2.2). Brancheau and Nansi (2001) described the following four main common reasons usually undertaken in insecurity of the Internet.

*First*, usually the client computer is insecure. If we are consumers dealing with e-commerce, this means our computers are insecure. When we do not have own password, the operating system does not enforce stringent security discipline, we do not encrypt our local files and also we ever let anyone else use our computer, our computers are not secure. If we are web vendors, this means our consumers' computers are insecure. We do not necessarily know who was using that computer even if we know that a message originated from a specific computer.

*Second*, many client computers and web servers are attached to a Local Area Network (LAN). Employees within an organization can easily eavesdrop on LANs. The Ethernet protocol that is standard on most LANs uses a broadcast technology.

This means that all computers on the local network receive all messages, whether they are intended for that computer or not. Normally, each computer ignores all messages except those intended for it. This system can be compromised by anyone who knows a bit about network design.

*Third*, the intermediate networks comprising the Internet are public and open. This is good because it radically reduces their costs. This is bad, however, because these networks are not necessarily owned or operated by someone we trust. Messages traversing the Internet usually pass through many different intermediate networks. Routers are switches that were built to operate the internetting layer. The Internet uses routers to interconnect millions of host computers across thousands and thousands of these intermediate networks. Routers at each network connection temporarily store our data packets before forwarding them to the next network. Dishonest operators can set up listener programs to pull off packets and reassemble them into complete messages.

*Fourth*, the Web server may be insecure due to its operating system or lack of effective management. Many Web servers are located on a LAN inside a firewall. The LAN connects many host computers together. Once the Web server is compromised, the attached LAN is also compromised. Other hosts on the same LAN may contain sensitive corporate information, including customer credit card numbers, purchasing patterns and pricing information.

- Client is usually insecure.
- LANs are easy to eavesdrop on.
- Intermediate networks are public and 'open'.
- Destination server may be insecure or spoofed

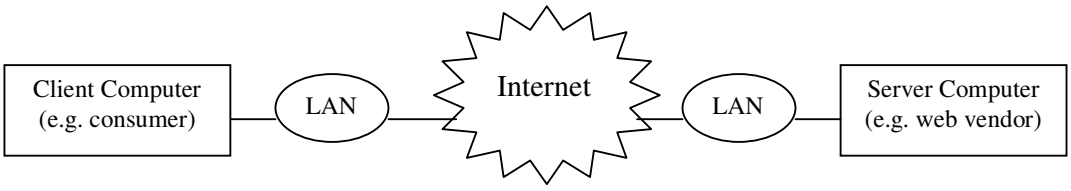



Figure 2.2. Why the Internet is Insecure (Brancheau and Nansi, 2001).

## 2.4 E-Commerce in Malaysia

Internet Usage and World Population Statistics for September 30, 2009 are shown in Table 2.1. Demographic (Population) numbers are based on data from the US Census Bureau. Internet usage information comes from data published by Nielsen Online, by the International Telecommunications Union and other reliable sources (Miniwatts Marketing Group, 2009).

Table 2.1
World Internet Usage and Population Statistics (September 30, 2009)

| World Regions | Population ( 2009 Est.) | Internet Users Dec. 31, 2000 | Internet Users Latest Data (September 30, 2009) | Penetration (% Population) | Growth 2000-2009 | Users % of Table |
|---|---|---|---|---|---|---|
| Africa | 991,002,342 | 4,514,400 | 67,371,700 | 6.8 % | 1,392.4 % | 3.9 % |
| Asia | 3,808,070,503 | 114,304,000 | 738,257,230 | 19.4 % | 545.9 % | 42.6 % |
| Europe | 803,850,858 | 105,096,093 | 418,029,796 | 52.0 % | 297.8 % | 24.1 % |
| Middle East | 202,687,005 | 3,284,800 | 57,425,046 | 28.3 % | 1,648.2 % | 3.3 % |
| North America | 340,831,831 | 108,096,800 | 252,908,000 | 74.2 % | 134.0 % | 14.6 % |
| Latin America/ Caribbean | 586,662,468 | 18,068,919 | 179,031,479 | 30.5 % | 890.8 % | 10.3 % |
| Oceania / Australia | 34,700,201 | 7,620,480 | 20,970,490 | 60.4 % | 175.2 % | 1.2 % |
| WORLD TOTAL | 6,767,805,208 | 360,985,492 | 1,733,993,741 | 25.6 % | 380.3 % | 100 % |
| * Malaysia | 25,715,819 | 3,700,000 | 16,902,600 | 65.7 % | 356.8 % | 2.3 % |

At the year 2009 quarter 2, there were 704,213,930 estimated Asia Internet users, where as Malaysia ranked Ninth among Asia Top 10 Internet countries with estimated Internet users 16,902,600. List of Asia Top 10 Internet countries is shown in Figure 2.3.

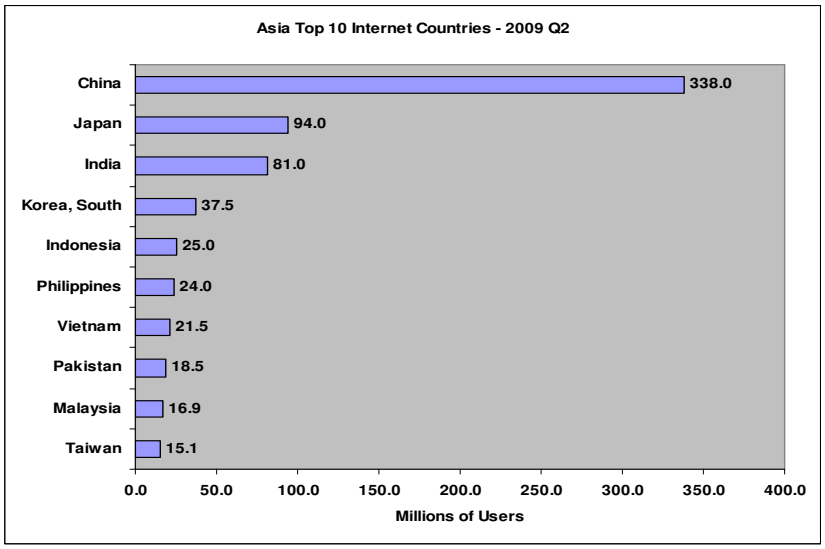



Figure 2.3. Asia Top 10 Internet Countries (2009 Q2).

Due to rising Internet penetration, e-commerce is fast catching up among Malaysian consumers. Based on IDC reports, in the year 2009, more than 8 million Malaysians (half of internet users population) have actually participated in e-commerce activities. Moreover, it is estimated that by the end of year 2010, Malaysian Internet users population will reach to 17.5 million and out of which, 8.9 million will participate in e-commerce activities, as shown in Figure 2.4.

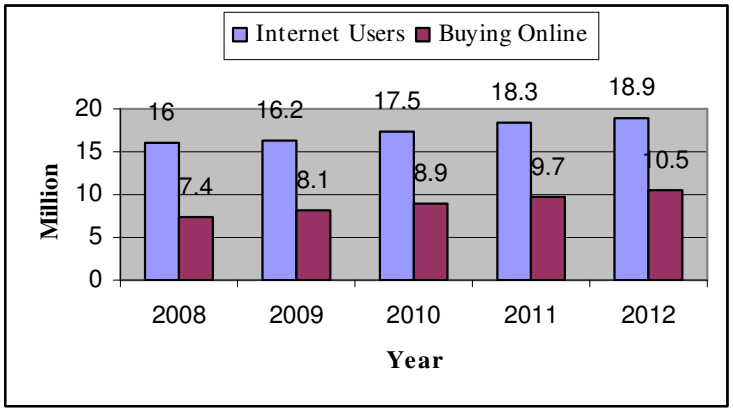



Figure 2.4. Internet Users VS Buying Online in Malaysia.

A survey conducted by the IDC's Skypad in 2008 reveals that among the nine countries surveyed in Asia Pacific who uses the Internet to purchase travel-related items, Malaysia ranks with the uppermost in percentage of online purchasers. Majority of Malaysian Internet users (about 82%) have purchased travel items online, followed by majority (about 69%) have purchased books over the Internet.

Nevertheless, CEO of Acmamall.com Sdn Bhd, Christopher Quek, mentioned that "Online stores which wish to be successful must be able to ride out the early stages. Consumers still like to see, touch and feel and generally take a long time to trust online stores in Malaysia". Another survey conducted by The Nielsen Company on online shopping habits with 500 Malaysian Internet users reveals that Malaysian Internet users (about 30%) have engaged in e-commerce transactions. The results also show that majority (about 55%) have involved in airline tickets and reservations, followed by about 41% (tour or holiday reservations) and about 22% (computer hardware). For the time being, about 18% of the surveyed Internet users have bought the event tickets online while about 21% have purchased books over the Internet (Yee and Seong, 2009). Figure 2.5 shows products or services bought online in Malaysia in 2008 based on IDC Malaysia report.

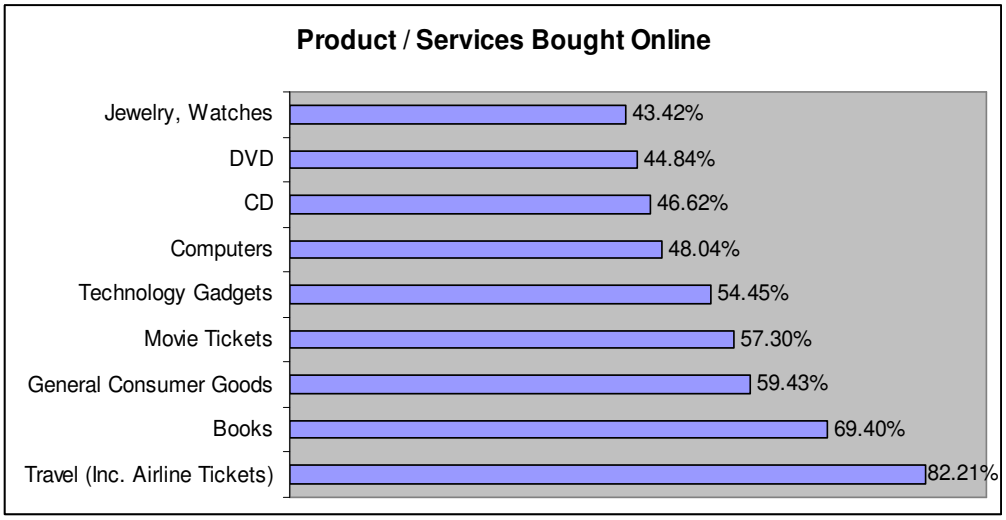



Figure 2.5. Products or Services Bought Online in Malaysia.

Some of the Malaysia's top e-commerce sites are: *Air Asia* – (Air Asia mainly started with internet being their major sales channel. In Malaysia, local e-commerce acceptance is being influenced with the emergence of Air Asia. So far, Air Asia is the biggest stimulator of local e-commerce activities since air ticket is the top item Malaysians are buying online.) *Lelong* – (Lelong has been around since 2000 in Malaysia, adopting eBay-like auction model, and claims to have 1 million visitors monthly. Lelong also has a Facebook-like social network site.)

According to a survey by eBay Southeast Asia, Malaysians are using eBay as a platform for entrepreneurship and cross border trading. The study revealed that 41% of eBay Malaysia members considered themselves serious sellers. Malaysians are either actively sourcing for products to sell on eBay or using eBay as the primary source of income.

Other interesting findings on eBay Malaysia are 75% are adults in the age group of 25 to 49, more than 60% are male, 84% use broadband, and the majority spend an average of 29 hours per week online, of which, seven hours are spent purchasing products or services on the Internet. Based on IDC Malaysia report, Figure 2.6 shows Malaysian online consumers by Age group in 2008. The report shows that most of the Malaysian online consumers are contributed by the working adults. Almost 60% of online consumers' professions are managers or executives and 13% of them are students.

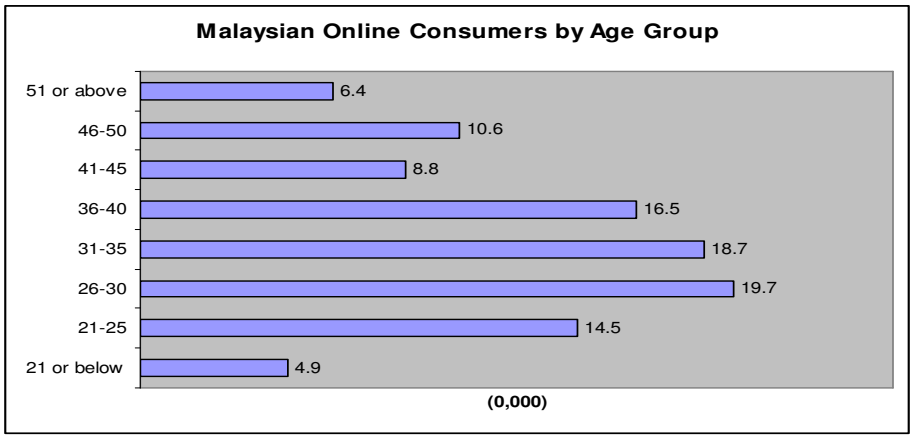



Figure 2.6. Malaysian Online Consumers by Age Group.

Malaysians buyers are also very active, spending close to one third of their time online browsing for goods and services on the auction website. Moreover, 42% visit eBay once to three times a week. The most frequently purchased items on eBay Malaysia are clothing, shoes and accessories (about 38%), followed by books (about 36%) and computers and networking services (about 34%). The visitors surveyed on the local website were generally affluent and well-educated with 64% having completed tertiary education and 75% earning at least RM20,000 per year. In addition, Malaysian shoppers spent approximately RM411 on average with eBay, out

of the total RM542 spent online. Credit cards were the most common payment method, followed by PayPal.

## 2.5 Summary of Prior Researches and Literature on E-Commerce Adoption

This section presents a summary of important studies and literature reviews that have been undertaken on security, privacy, trust, risk, and e-commerce adoption. There seems to be many studies related to security and privacy, trust beliefs of web vendors and Institutional trust, consumers' trust and their risk perceptions related to e-commerce transactions. These concepts of security, privacy, trustworthiness of web vendors, and risk perceptions are applied for many aims together with several senses. It is essential to know that these concepts give diverse purposes. For instance, though security is generally employed to technical concept, trust and risk are individual associated concepts. Therefore, security in this sense can be considered as the means to achieve and supporting the consumers' privacy in dealing with e-commerce.

### 2.5.1 Perceived Security and Perceived Privacy

While talking about trustworthiness of e-commerce transactions, many researchers study the security and privacy issues (Florian, 2001). Perceived security can be defined as consumers' beliefs about their sensitive personal information which will not be altered during information transfer and will not be able to receive by unintended third parties. Consumers' concerns on security issues become one of the major barriers to adopt e-commerce transaction (Kai et al., 2004).

Bush and Harris (1998) stated that security and privacy issues were the main barriers in e-commerce. According to Gervey and Lin (2000), security was one of the most essential concerns in order for consumers to trust in commerce transactions. The study based on 158 respondents reported that security and privacy concerns were found to be a major barrier to online shopping, and the users are also concerned about the safety and confidentiality of their e-mails (Godwin, 2001).

Considerable numbers of research findings (Dong-Her et al., 2004; Chou et al., 1999; Furnell and Karweni, 1999) stated that consumers' perceived security is one of the major barriers to the growth of e-commerce. According to Sara et al. (2000), one of the reasons is the probability of consumers' monetary and sensitive personal information may be interrupted for the purpose of fake use. According to the researchers, consumers' concerns about the consistency of the techniques used for online payment and information transmission methods and being stored is reflected by security (Kolsaker and Payne, 2002).

A study by Yang and Jun (2002) revealed that security was the main concern for a consumer who decides not to engage in e-commerce transaction. Salisbury et al. (2001) found that consumers' perceived security was a main obstacle to transact in e-commerce compared to perceived ease of use and online store site's usefulness. The authors defined consumers' security concerns as one's beliefs that online store sites will not be able to protect the business transaction information from security breaches during transit and being stored.

Looi (2005) found that, in Brunei Darussalam, the ranking factors in terms of relative importance, namely, competitive pressure, IT knowledge, relative advantage, security and government support, and the effects of these factors describe more than fifty per cent of the difference in SMEs adoption. The study of 190 students and 75 non-students to investigate on general online purchasing behavior of individual consumers and why they choose to buy or not buy online by Ahuja et al. (2003) found that security and privacy concerns were the single greatest barriers to online commerce. In addition, the authors stated that security and privacy factors were found to be more important than price.

While security concerns can be classified as 'environmental control', privacy concerns can be 'control over secondary use of information' (Belanger et al., 2002). According to the authors, the use of security controls is related to environmental control in e-commerce transactions that secure the transmission of consumers' financial and sensitive personal information during the transit. Hoffman et al. (1999a) stated that environmental control is the consumers' abilities to manage the actions of others in the e-commerce environment during in exchange of commercial transaction.

In addition, the authors (Belanger et al., 2002 and Hoffman et al., 1999a) agreed that environmental control attempted to ease consumers' concerns as regards to their sensitive personal information provided to online store sites from the fear of stealing their identities by hackers for unintended misuse of their sensitive personal information.

A study by Pavlou and Chellappa (2001) also found that perceived security was more important although perceived privacy was a major contributor to consumers' trust. The empirical study by (Belanger et al., 2002) confirmed that security concerns would be more important than privacy concerns from consumers' point of views. Laforet and Li (2005) investigated that the issue of security was found to be the most important factor that motivated consumers' adoption of online banking in China.

The study based on a survey conducted with 231 offline and 311 online buyers showed that poor customer service, concerns about online privacy and security prevented many consumers from shopping online. The results also indicated that consumers in general believed that online companies shared their sensitive personal information with other businesses (Lepkowska, 2003). The consumers' beliefs revealed that their sensitive personal information could be gathered easily by web vendors over the Internet (Graeff and Harmon, 2002). The study by Das et al. (2003) revealed that consumers' security concerns were higher when they had low interpersonal trust in dealing with e-commerce transactions.

The survey by Norhayati (2000) to 57 various companies in Klang valley revealed that about 70% of the respondents believed that security aspects were the most important barriers to e-commerce development in Malaysia. According to the author, the three aspects of security that respondents worry were: concerns for payment details such as credit card number, unauthorized access to their computer by hackers and the privacy of potentially commercial sensitive information sent over the Internet. In addition, uncertainty surrounding contractual and financial issues were also important barriers to the expansion of e-commerce. Mustafa and Mohd Khairuddin (2003) and Yusof and Mohd Yusof (2005) also stated that the lack of security and reliability as the most concerned barriers to e-commerce adoption in Malaysia.

Liao and Cheung (2003) noted that transaction security was likely to emerge as the biggest concern among the e-bank's account holders. A study by Dauda et al. (2007) studied the Internet banking adoption in Malaysia and Singapore, and found that consumers' perceived trust, relative advantage, Internet experience, non-repudiation, and banking needs were the most significant factors that affected Internet banking adoption in Malaysia.

A survey of 222 Malaysian industries by Khatibi et al. (2003) investigated that the concern on security and privacy issues was one of the major barriers for the adoption of e-commerce, from the web vendors' point of view. Ainin (2000) found the issue of security was the major obstacle to the implementation of e-commerce in Malaysia. The author also stated that Malaysian industries were hesitant to implement e-commerce strategies as they considered that the commercial transactions between consumers and web vendors were open to viruses and hackers, which could not be controlled easily by web vendors.

Ahmed et al. (2007) revealed that from the Malaysian consumer's opinions, the key concerns for the adoption of e-commerce were: security and privacy of their sensitive personal information during transit and storage, and trustworthiness of web vendors. They suggested that web vendors needed to give much effort to ensure that consumers' concerns on security and privacy of their sensitive personal information were adequately controlled in order to successfully implement e-commerce in Malaysia. An expert mentioned that, in Malaysia, the e-commerce market growth rate was 70% in 2006 compared with that in 2005. Nevertheless, there are still lots of work to be done for e-commerce growth and development. (Lincoln Lee, Senior Analyst, Telecommunication Research, IDC Malaysia).

The study by Tamura (2003) stated that the security level of society would rise if organizations defined the individual's responsibility regarding a "culture of security". Moreover, for the online business, control of executives is essential for the success of online security. According to Jawahitha (2004), online consumers will not be getting sufficient safety, in Malaysia, until the Malaysian government takes steps to modify some of the present laws to deal with the issues in e-commerce sufficiently.

With the revolution of World Wide Web, the issue of privacy has become major concern with the implementation of e-commerce (Nugent and Raisinghani, 2002). According to Malhotra et al. (2004) and Yousafzai et al. (2003), trust is influenced by consumers' perceived security and perceived privacy. Malhotra et al. (2004) also stated that consumers' concern on privacy issues was influenced as a main barrier to e-commerce growth.

In most of the privacy literatures, security and privacy concerns are assumed as a single construct (Liu et al., 2004 and Belanger et al., 2002). However, Chang et al. (2005) and Vijayasarathy (2004) agreed that security and privacy concerns were two different factors. Security and privacy have to be regarded dissimilar because, in reality, an online store site might be somewhat adapt at securing consumer's sensitive personal information in transit, but web vendors might freely share it with unintended third parties freely (Michael, 2007). The studies found that the concern on privacy issues were higher compared to the concern on security issues (Paola, 1999). This may be because consumers are so worried that how their sensitive personal information will be used and handled by web vendors.

Wherever the internet is pertained, consumers are so concerned on privacy issues, such as gathering, storage, sharing or the misuse of their sensitive personal information (Wang et al., 1998). Kelly and Erickson (2005) stated that the advent technologies for transaction processing had caused privacy gradually more important matter. As a result, consumer distrustfulness is rising regarding how their sensitive personal information is being collected, processed and distributed. Lanier and Saini (2008) noted that consumers had concerned privacy of their sensitive personal information, and they had always wanted control on the exposure of their sensitive personal information. This can be said that consumers' privacy concerns have always presented since primitive society and are not new to today modern society. However, the appearance and way of privacy and its safety have transformed in today society. For example, in traditional commerce, consumers' sensitive personal information was protected as expected and not available for privacy breaches because they did not have to provide their sensitive personal information to offline vendors. In addition to increasing trust, Hann et al. (2007) stated that web vendors should offer incentives to their consumers in order to decrease their consumers' concerns on privacy issues

related to financial and sensitive personal information in dealing with e-commerce transactions.

A study of privacy and data Protection by Munir, in 2003, indicated that Malaysian consumers, in general, did not like if web vendors used their sensitive personal information for advertising exclusive of their permission, particularly when sensitive personal information was distributed to other third parties for unintended purposes. The consumers on privacy issues are utmost in the e-commerce market environments and consumers always want to get control over their sensitive personal information and how it is being gathered and treated. Privacy concerns affect the way in which consumers act and deal with e-commerce transactions since there is a extremely high level of consumers' concerns on privacy issues.

Ida (2002) studied the scope, manner, and nature of personal data protection bill invented by Malaysian legislators in order to care for e-commerce consumers' privacy, and found that it only dealed with the way consumers' sensitive personal information was being gathered, storage, analysed, and distributed rather than complete concerned surveillance and privacy issues. Carlos and Miguel (2006) stated that consumers' trust in e-commerce was mainly influenced by their perceived security concerning the managing and usage of their sensitive personal information.

The study based on an e-mail survey by Swaminathan et al. (1999) showed that consumers who frequently purchased online were concerned on formation of new laws defending privacy in dealing with e-commerce transactions. In addition, consumers believe that web vendors do not have to ask for more information about their consumers to effectively market products and services over the Internet. Hawkins et al. (2001) reported that online thief used emerging information technologies as a means for their own gain, i.e. stealing and misusing of consumers' sensitive personal information. Moreover, web vendor has to protect privacy on the Internet by utilizing emerging information technologies, such as, to protect consumers' sensitive personal information during transit, ensure the identity of a legitimate user, and protect the consumers' sensitive personal information from unauthorized access.

Indeed, the advent of technological capabilities has helped for gathering, storing and distribution of consumers' sensitive personal information speedily. Anonymity has faded away with the innovation and development of e-commerce (Caudill and Murphy, 2000), and media exposure on consumer privacy issues along with the government regulation for increased privacy concerns are leading to consumers to concern more and more about their sensitive personal information (Roznowski, 2003). Olkowski (2001) indicated the forewarning signs for e-commerce from the professional thief or hacker. The author hopped that more awareness on this problem would result in the growth and development of successful e-commerce.

Cheung and Lee (2001) found that consumers' perceived privacy control and perceived security control were significant factors influencing the growth of consumers' trust in e-commerce transactions. Luo (2002) suggested that institutional trust, i.e. banks, credit card companies, had the potential to increase consumers' trust by reducing their concerns about privacy of sensitive personal information. According to the author, privacy is no more barrier to the formation of trust due to the current development of institutional trust mechanisms.

A study by Mozilo (2001), reported that majority (about 72%) of the respondents were so much concerned on privacy of their sensitive personal information in dealing with e-commerce transactions while majority (about 92%) of the participants were concerned on overall online privacy. Graeff and Harmon (2002) later found in the phone survey study, majority (about 75%) of the respondents were felt uneasy to disclose their credit card information to web vendors. However, Rust et al. (2002) argued that consumers' privacy concern would be almost disappeared over time since they must have to disclose their sensitive personal information in order to gain the benefits offered by e-commerce.

A study revealed that consumers were uncomfortable to disclose their sensitive personal information to web vendors (Hoffman et al., 1999; and Phelps et al., 2000). According to Hoffman et al. (1999), majority (about 94%) of the respondents, sometimes, had declined to reveal their sensitive personal information to web vendors. The authors also stated that of the respondents who had disclosed their demographic information to web vendors, about 40% of the respondents actually had

provided fake information. Phelps et al. (2001) stated that most of the consumers were so concerned to disclose their sensitive personal information. However, a study found that majority of the respondents (approximately 86%) were eager to provide their sensitive personal information, such as names and addresses to the web vendors (Ward et al., 2005).

The survey of 86 respondents from HR industry and IT industry by Martins et al. (2001) reported that consumers are reluctant to reveal their sensitive personal information when dealing with e-commerce transactions due to the hacker and safety concerns as the major reason, in general. Moreover, the authors stated that respondents (from the Human Resource department) were unwilling to give their sensitive personal information compared to respondents (from the Information Technology Department) in engaging in e-commerce transactions, and the respondents (from the Human Resource Department) were less aware of and educated about information security measures compared to respondents (from the Information Technology Department) in engaging in e-commerce transactions

Sheehan and Hoy (2000) stated that the major influences on the degree to which consumers had privacy concerns were due to the awareness of information gathering and handling beyond the original transaction. Stewart and Segars (2002) validated the measure based on four dimensions, namely, improper access, unauthorized secondary use, collection, and errors, to handle consumers' concerns on information privacy practices prepared by organizations. Malhotra et al. (2004) studied online consumers' information privacy concerns that consisted of three dimensions, namely, collection, control and awareness.

Moores and Dhillon (2003) noted that many existing commercial web sites did not contain any kind of privacy declaration statement. According to the authors, the virtual success of the privacy seals (TRUSTe, Web Trust, and BBBOnline) recommends that many online store sites be aware of the privacy issues and attempt to maintain the highest standards. However, the perceptions by consumers will maintain to be that hackers hang around over the Internet to steal their sensitive personal in dealing with e-commerce transactions. These perceptions result in slow growth of e-commerce.

Sipior et al. (2004) indicated that consumers' privacy related to ethical issues over the Internet, namely, loss of anonymity, unintended uses of consumers' sensitive personal information, information sharing, direct marketing and so on were hindering consumers from dealing with e-commerce transactions. According to the authors, protecting consumers' privacy is both economic and ethical issue, and in order to promote the growth and development of e-commerce, it is essential to deal with the protection of consumers' concerns on privacy issues. Metzger (2004) indicated that the web vendor might have a mostly strong effect on disclosure, both independent of, and mediated by, trust. The findings also suggested that online store sites had to be responsive to consumers' concerns on privacy issues and to discover ways to correspond this sensitivity on their online store sites.

Phelps et al. (2001) revealed that consumers' major concern was control over how their sensitive personal information would be used by web vendors, while the authors studied the four factors (i.e. What kinds of consumers' sensitive personal information, How much control that consumers were devoted to use over their sensitive personal information, the possible outcomes and advantage for consumers, and the consumers' attributes related to privacy concerns, in general) which influence consumers' privacy concerns, in 2000. Culnan and Armstrong (1999) revealed that consumers' trust in e-commerce transactions was built by organisational fair practices relative to their sensitive personal information.

Cary et al. (2003) and Milne and Rohm (2000) mentioned that consumer privacy categories could be the course of actions, such as web browser cookies, website registration forms, the gathering and handling of the consumers' sensitive personal information by web vendors. Chellappa and Sin (2005) stated that the groups of consumer privacy might be established based on e-commerce involvement, their relationships with web vendors and individuals' characteristics. An empirical study of 809 consumers from the U.S.A and India, to explore the revealing behaviour of their sensitive personal information and their aims to obtain and carry out protective measures in dealing with e-commerce transactions, found that US consumers intended to and engaged in higher passive privacy protection actions compared to Indians, and Indian consumers were more eager to reveal potentially sensitive personal information (Babita et al., 2010).

Liu et al. (2004) stated that notice, access, choice and security were four attributes privacy which determined consumers' trust in e-commerce transactions, an, Lanier and Saini (2008) stated that consumers' privacy concerns regarding e-commerce transactions could be categorised into three groups. However, a survey of online consumers by Saunders (2004) reported increasing consumers' trust in e-commerce transactions. The researcher stated that one of the reasons handed by consumers for their increasing trust in e-commerce transaction was that consumers were getting smarter in dealing with e-commerce transactions regardless of their privacy concerns.

A study reported that the Internet frequent users expressed less privacy concerns toward the e-commerce transactions while the Internet seldom user appeared to be so concerned on privacy of their sensitive personal information (Lynch and Beck, 2001). It is supported by Miyazaki and Fernandez (2001) that the Internet frequent users concerned less on the privacy of their sensitive personal information in dealing with e-commerce transactions. However, study by Hoffman et al. (1999) revealed that consumers' privacy concerns on their sensitive personal information boosted up with the individual user's online skill capability.

Even though the security and privacy in online environments are linked together, they have detailed attributes that can be established an obvious differentiation among them. Particularly, privacy is related to a set of good practices and authorized requirements with regard to the managing of consumers' sensitive personal information, for example, web vendors should inform the consumer that what type of consumers' information are going to be gathered and how they will be treated at the time of engaging in e-commerce transactions. On the other hand, security refers to the technical guarantees that ensure that the legal requirements and good practices with regard to privacy will be effectively assembled (Carlos and Miguel, 2006). For example, the web vendor might promise that without the consumer's knowledge or consent, the collected consumers' sensitive personal information will not be distribute to unauthorized third parties.

Belanger et al. (2002) stated that privacy issues on the Internet included the sharing of information with third parties. The studies demonstrated that perceived risk in internet banking was mostly influenced by security, privacy, performance and

finance concerns (Aldas et al., 2009, Littler and Melanthiou, 2006; and Yousafzai et al., 2003). Moreover, Aldas et al. (2009) stated that the security and performance of banking transactions, and the confidentiality of personal account data were identified as common concerns. While Sergios and Nikolaos (2010) tested a model that combined the effect of trusting beliefs and trusting intentions together with the Technology Acceptance Model variables, security, privacy, and individual attributes, 762 retail bank consumers exposed a strong mediating role of trusting intention on the intention to use and similar patterns of association for the two technology-based bank channels.

The relationship between the concepts of security and privacy might be found closely in specific areas, such as public bodies might view both concepts as running alongside and also web vendors be likely to hold both concepts together. Even though, both consumers and web vendors perceive that security and privacy concepts have a close relationship, the two should be considered different concepts due to the distinctiveness of the security and privacy variables,.

The security of an electronic commerce transaction can be scientifically assured with third party authentication, digital signatures and adequate encryption. However, the different views on the definition of privacy (i.e. the right to be let alone, control over personal information, a form of personhood protection, secrecy, intimacy and so on), make online privacy more difficult to create. The terminology about privacy keeps changing in research domains, and academic literature uses terms such as information privacy, consumer online privacy, privacy concern, perceived privacy and so on.

In summary, the researches mentioned have approved the consumers' concerns on security and privacy issues related to their trust in e-commerce transactions. Almost all of the researchers agreed that consumers concerned the security and privacy issues toward e-commerce transactions, in reality. In order to achieve the growth and development of e-commerce, it is essential for web vendors to control and manage the security and privacy concerns of their consumers.

The selected prior researches on security and privacy concerns related to e-commerce adoption are exhibited in Table 2.2(i) and Table 2.2(ii).

Table 2.2(i)
The Selected Prior Researches on Security and Privacy Concerns

| Author(s) | Findings |
|---|---|
| Bush and Harris (1998) | Security and privacy issues were the main barriers in e-commerce. |
| Paola (1999) | The concern on privacy issues were higher compared to the concern on security issues. |
| Gervey and Lin (2000) | Security was one of the most essential concerns in order for consumers to trust in commerce transactions. |
| Norhayati (2000) | The survey of 57 various companies in Klang Valley revealed that about 70% of the respondents believed that security aspects were the most important barriers to e-commerce development in Malaysia. |
| Salisbury et al. (2001) | Consumers' perceived security was a main obstacle to transact in e-commerce compared to perceived ease of use and online store site's usefulness. |
| Pavlou and Chellappa (2001) | Perceived security was more important although perceived privacy was a major contributor to consumers' trust. |
| Godwin (2001) | The study based on 158 respondents reported that security and privacy concerns were found to be a major barrier to online shopping, and the users were also concerned about the safety and confidentiality of their e-mails. |
| Cheung and Lee (2001) | Consumers' perceived privacy control and perceived security control were significant factors influencing the growth of consumers' trust in e-commerce transactions. |
| Yang and Jun (2002) | Security was the main concern for a consumer who decided not to engage in e-commerce transaction. |
| Belanger et al. (2002) | Security concerns would be more important than privacy concerns from consumers' point of views. Privacy issues on the Internet included the sharing of information with third parties. |
| Ahuja et al. (2003) | Security and privacy concerns were the single greatest barriers to online commerce. In addition, security and privacy factors were found to be more important than price. |
| Liao and Cheung. (2003) | Transaction security was likely to emerge as the biggest concern among the e-bank's account holders. |
| Khatibi et al. (2003) | The concern on security and privacy issues was one of the major barriers for the adoption of e-commerce, from the web vendors' point of view. |
| Das et al. (2003) | Consumers' security concerns were higher when they had low interpersonal trust in dealing with e-commerce transactions. |
| Lepkowska (2003) | The study based on a survey conducted with 231 offline and 311 online buyers showed that poor customer service, concerns about online privacy and security prevented many consumers from shopping online. Moreover, consumers in general believed that online companies shared their sensitive personal information with other businesses. |

Table 2.2(ii)

The Selected Prior Researches on Security and Privacy Concerns

| Author(s) | Findings |
|---|---|
| Mustafa and Khairuddin (2003) | The lack of security and reliability as the most concerned barriers to e-commerce adoption in Malaysia. |
| Kai et al. (2004) | Consumers' concerns on security issues were of the major barriers to adopt e-commerce transaction. |
| Malhotra et al. (2004) | Consumers' concern on privacy issues was influenced as a main barrier to e-commerce growth. And trust was influenced by consumers' perceived security and perceived privacy. |
| Laforet and Li (2005) | The issue of security was found to be the most important factor that motivated consumer adoption of online banking in China. |
| Carlos and Miguel (2006) | Consumers' trust in e-commerce was mainly influenced by their perceived security concerning the managing and usage of their sensitive personal information. |
| Ahmed et al. (2007) | From the Malaysian consumer's opinions, the key concerns for the adoption of e-commerce were: security and privacy of their sensitive personal information during the transit and storage, and trustworthiness of web vendors. |
| Hann et al. (2007) | Web vendors should offer incentives to their consumers in order to decrease their consumers' concerns on privacy issues related to financial and sensitive personal information in dealing with e-commerce transactions. |
| Lanier and Saini (2008) | Consumers had concerned privacy of their sensitive personal information, and they had always wanted control on the exposure of their sensitive personal information. |
| Aldas et al. (2009) | Perceived risk in internet banking was mostly influenced by security, privacy, performance and finance concerns. |
| Babita et al. (2010) | U.S consumers intended to and engaged in higher passive privacy protection actions compared to Indians, and Indian consumers were more eager to reveal potentially sensitive personal information. |

### 2.5.2 Trustworthiness of Web Vendors

Trustworthiness of web vendors has been recognized as one of the essential factors to reduce consumers' concerns on security and privacy issues related to their sensitive personal information in dealing with e-commerce transactions. Therefore, trust is necessary to e-commerce, and the issue of trust is essential for secure e-commerce. According to Tang et al. (2003), trust is the foundation upon which commerce is built and it may be even more important in online transactions compared to offline

transactions. In various literatures concerning with trustworthiness of web vendors, for both traditional and electronic commerce, there is no agreement on the "true" definition of trust (Cynthia et al., 2001). The lack of agreement on one definition could stem from the idea that trust is a many-sided concept (Deepak et al., 2002 and Cynthia et al., 2001). Deepak et al. (2002) formulated a framework to understand the practices and behaviours of service providers that constructed or reduced consumers' trust and the methods that changed the consumers' trust into value and loyalty in relative exchanges. The authors tested the proposed framework based on two service contexts, i.e. retail clothing (N = 264) and non-business airline travel (N =113).

Trust is a complicated element to define (Russell, 2001). This may be due to interchanging terms like trust, trustworthiness, trusting or entrusting. Consumers might fear revealing sensitive personal information to web vendors, merely because they do not have enough trust to engage in e-commerce transactions involving financial and sensitive personal information (Salam et al., 2003, So and Sculli, 2002; Hedelin and Allwood, 2002 , Gefen, 2000; and Jarvenpaa et al., 2000). According to Russell (2001), the longer the relationship between consumers and web vendors, the more trustworthy and dependable parties turn out to be.

A study by Tan and Sutherland (2004) treated trust as a multidimensional factor including three elements, namely, interpersonal, institutional, and dispositional trust, with the concern on consumers' trust on e-commerce transactions. The study by Heuvelmans (2000) highlighted the inherent relation between security, privacy, and trust, that is, online consumers had to trust the web vendors to provide a truthful service, and not to mishandle their sensitive personal information they provided. It can be assumed that trust is the foundation of e-commerce, and security measures provide a basis for trust.

Trust is promising as a key element of success in the online surroundings. Many studies have exposed that trust is the means to the growth and achievement of e-commerce transactions (Florian, 2001 and Eric, 2000). The findings by Carlos and Miguel (2006) suggested that the enlargement of trust affected both the consumers' intentions to purchase, and the effective purchasing behaviour, in terms of frequency of visits, cost and preference, and thus, the level of productivity provided by each

consumer. Salam et al. (2003) stated that trust acts as an important role in many electronic transactions. Trust is a vital issue in individual relationships (Justine and Timothy, 2000) and the issue of online trust is essential as well (David, 2002 and Yao-Hua and Walter, 2000). According to David (2002), trust and trustworthiness must not be observed as a single construct with a single effect. Relatively, different consumer activity intentions are influenced by different beliefs. Yao-Hua and Walter's thoughts revealed that if we did not know a control mechanism, i.e. the procedure and protocols related to e-commerce, then it was of little value to us and our trust in the control mechanism was then only based on a judgement by another party. Sara et al. (2000) presented the framework that assisted in thoughtful of the implications of new e-business issues for traditional concepts of dependability and trust. According to Rohit and Adam (1998), trustworthiness of web vendors is an essential concern for e-commerce. David (2002) mentioned that online store sites would be more successful if consumers trusted more on web vendors in dealing with e-commerce transactions.

Jakob (1999) stated that trust was resulted from web vendors' actual behaviours toward their consumers experienced over an extended set of encounters, while Judith (2000) stated that "People learn to trust others by noting their behaviours. Promising to do something and fulfilling the promise earns trust. Interestingly, people can also engender trust by making themselves vulnerable, inviting others to trust them, because they themselves are so trusting (p.43)". Eric (2000) mentioned that trustworthiness of web vendor was important, but how this trust plays was not yet entirely realized. Justine and Timothy (2000) stated that trust promoted cooperative behaviour. This is agreed by Batya et al. (2000) that a mood of trust eases collaboration between people and people trust people, not technology. However, Russell (2001) stated that an individual could deal with online vendor involving financial and sensitive personal information, not because he/she trusted web vendor but because he/she had no options. According to the author, trust seems to be a primitive, unanalyzed term and if something conceptually causes or involves trustworthiness, and then it tends to cause trust indirectly. In addition, the author mentioned that trust was essentially a matter of knowledge or belief and it was

essential to make a note that there was no risk in trusting alone, the risk was in acting on trust.

Head and Hassanein (2002) studied the impact of trusted third party referees' seals of approval as intermediaries to build consumers' trust in dealing with e-commerce transactions, by developing a model for online consumers' trust. Trustworthiness of web vendor can eliminate consumers' risk concerns in dealing with e-commerce transactions (Salam et al., 2003 and Sara et al., 2000). Trust can be viewed as a complicated social phenomenon reflecting social, behavioural, technological, psychological and organizational interactions among individual and non-human technological agents (Salam et al., 2005). David (2002) proposed a three-dimensional scale of trustworthiness regarding with ability, benevolence, and integrity in dealing with consumers' trust in e-commerce transactions, and then showed the significance of investigating the consequences of each dimension individually. Trust can be used to overcome vulnerability (David, 2002; Cynthia et al., 2001 and Batya et al., 2000), as well as uncertainty (Grabner, 2002). According to Deepak et al. (2002), the motivation and intentions of a trusted party have an effect on his/her level of trustworthiness while there are significant payoffs from building consumer trust in relational exchanges, realizing them is neither straightforward nor expected.

Miers (2003) mentioned that, in the online environment, the consumer would almost certainly know more about web vendor than the web vendor knew about the consumer. According to the author, if the trust relationship is accurate, they quickly become active partners and advocate, i.e. introducing new customers without further encouragement from the web vendor. The findings from a sample of 265 subjects faced with the decision of buying a travel package from an unknown online travel agency showed that association and similarity with a known brand are factors that promote consumers' trust and behavioural intentions (Elena and Miguel, 2008). A study by Kwek et al. (2010) with 242 undergraduate information technology students from a private university in Malaysia revealed that desired purchase intention, quality orientation, brand orientation, online trust and prior online purchase experience were positively related to the customer online purchase intention.

According to Xiaowen and Gavriel (2003), consumers would not automatically engage in e-commerce transactions, even though web vendors implemented perfect systems for completely secure e-commerce transactions. Salam et al. (2003) stated by judging that secure technological infrastructure was only a basic foundation and by itself not adequate for building the level of trust needed for the growth and development of e-commerce transactions. According to Basu and Muylle (2003), both online consumers and web vendors require to obtain authentication information about each other and confirm the trustworthiness of this authentication information. The authors suggested that quality authentication mechanisms had to be developed that merged anonymity with the advantages of mutually beneficial buyer-seller, trusting, and long-term, relationships. The findings from two experimental studies of eBay users showed that trustworthiness judgments were influenced by the text comments associated with negative feedback and also by whether a trust violation was perceived as competence-based or morality-based (Sonja et al., 2009).

When discussing about online trustworthiness, context is important (Russell, 2001). Due to the diverse context of online or offline, trustworthiness in e-commerce is different than trustworthiness with regards to traditional commerce. Context can also be applicable to the different types of products being offered by online store sites. Some of the products, such as CDs, software and books, can be sold more easily online than others. This may be because these products descriptions can be easily provided more precisely and exactly on the online store sites.

Trustworthiness is a key component to credibility (Fogg et al., 2001), and trustworthiness of web vendors' actions can give the results of positive reputations (Grabner, 2002). According to the author, a web vendor's reputation can result how the consumer is willing to make a purchase. Russell (2001) described reputation as perceived trustworthiness. Reputation and credibility can be associated with brands. Xiaowen and Gavriel (2003) stated that consumer's trust in online store sites was influenced by brand names, which could be measured as one of the key factors in dealing with e-commerce transactions. A Quality-Purchase Interaction Model (QPI Model) of e-commerce for developing countries, developed by Shareef et al. (2008), indicated that on-line purchase decision was considerably influenced by perceived

customer value, perceived customer care, perceived site security, perceived trustworthiness and perceived operational security.

The study of non-random gender-balanced sample of 150 participants by Kolsaker and Payne (2002) provided that consumers' trust was a significant issue in e-commerce and they were so concerned about trust-building elements in dealing with e-commerce transactions. In addition, the results showed high levels of concerns for confidentiality of information, security of payment, and very high levels of concerns for web vendors' integrity. The empirical results from a survey of 140 online auction sellers at uBid.com found that system quality, information quality, and service quality affect relationship quality significantly, and in turn, relationship quality had major impact on customer retention and customer commitment (Heshan, 2010).

The design of the online store site can influence trustworthiness of an e-commerce store site (Xiaowen and Gavriel, 2003 and Katherine, 1999). Trustworthiness of web vendors can be influenced by the direction of visual elements in the online store sites' interfaces (Cynthia et al., 2001), and trustworthiness of web vendors can be negatively affected by the online store site's quality, such as, the website has typing error, link is not working properly and so on (Xiaowen and Gavriel, 2003 and Florian, 2001). A study found that new online store sites might profit from an overall integration effect when a link to their store sites was surrounded by links to more well-known online store sites, and well-known online store sites might profit from a contrast effect when new consumers saw their store site link surrounded by links to new online store sites (Katherine and Ross, 2009). Consumers draw on cues from the interface of online store site to decide the web vendor's purposes and their liabilities (Jens, et al., 2003; and Batya et al., 2000). One of the essential elements of the trustworthiness of the web vendors is the comparative ease of use (Florian, 2001; and Jarvenpaa et al., 1999). Therefore, it is important to design the interface of online store site to have strong and effective navigation in order to gain consumers to trust in web vendors, and in turn, trust in e-commerce transactions.

Nam et al. (2006) stated that the increased on consumers' trust in e-commerce and the benefit e-commerce offered to consumers were two key factors to reduce consumers' concerns on privacy of their sensitive personal information. The authors

recommended that in order to gain a certain degree of benefit from web vendors, consumers might be excited to reveal their sensitive personal information willingly to web vendors. Belanger and Carter (2008) integrated trust of the Internet, disposition to trust, perceived risk, and trust of the government in a model of the adoption e-government, and the authors found citizens were unwillingly to adopt e-government services due to a lack of trust. Therefore, trustworthiness of web vendors is important for the e-commerce to be successful.

The findings suggested that products that started with a highly rated brand were more likely to have additional reviews posted than products with an initial poorly rated brand (Naveen and Tung, 2008). Hann et al. (2007) suggested that web vendors could provide adequate privacy policies in their online store sites, and their intensions on the collection and distribution of consumers' sensitive personal information in order to obtain increased value from their consumers. The findings revealed that during the early stages of trust formation, four positive reasons, i.e., interactive, knowledge-based, dispositional, and calculative were associated with higher trust in online recommendation agents (RAs) and two negative reasons, i.e., interactive and calculative and were associated with lower trust in RAs (Weiquan and Izak, 2008).

A study by Spiekermann et al. (2001) revealed that in order to get additional benefit from web vendors, lots of consumers would disclose their sensitive personal information willingly share to online store site. Batya et al. (2000) stated that individuals could transact with online store sites, but still not yet generally judged about whether the communications are dependable. All of us have own personalities that influence our judgment to trust on someone (Grabner, 2002), and these characters can consist of the gender, age, race, occupation, and so on (Katherine, 1999). Malhotra et al. (2004) stated that consumers' attributes and personalities, for example, age, race, occupation were important and experience with particular online store site would have an effect on an individuals' perceptions of conditions. A study found that young consumers would have a tendency to view more positive about the gathering of their sensitive personal information compared to older consumers (Graeff and Harmon, 2002). The authors also stated that female consumers revealed more concerns on privacy issues than men. Therefore, all of us are dissimilar and these dissimilarities can influence individuals' trust in e-commerce adoption.

In summary, consumers recognize that they can easily search for a good deal over the Internet, and thus, it is one of the main causes consumers deal with e-commerce transactions. Like traditional stores, online store sites also need to build strong relationship with their consumers in order to be successful in competitive online environment. With the use of emerging technology, online store sites basically have more potential and advantages than traditional stores.

The selected prior researches on trustworthiness of web vendors related to e-commerce adoption are exhibited in Table 2.3(i) and Table 2.3(ii).

Table 2.3(i)
The Selected Prior Researches on Trustworthiness of Web Vendors

| Author(s) | Findings |
|---|---|
| Justine and Timothy (2000); and Batya (2000) | Trust promotes cooperative behaviour. And a mood of trust eases collaboration between people and people trust people, not technology. |
| Russell (2001) | The author described reputation as perceived trustworthiness. And the longer the relationship between consumers and web vendors, the more trustworthy and dependable parties turn out to be. |
| Grabner (2002) | Trustworthiness of web vendors' actions can give the results of positive reputations, and a web vendor's reputation can result how the consumer is willing to make a purchase. |
| David (2002) | Online store sites will be more successful if consumers trust more on web vendors in dealing with e-commerce transactions. |
| Tang, et al. (2003) | Trust is the foundation upon which commerce is built and it may be even more important in online transactions compared to offline transactions. |
| Salam et al. (2003) | Trust acts as an important role in many electronic transactions. Consumers might fear revealing sensitive personal information to web vendors, merely because they do not have enough trust to engage in e-commerce transactions involving financial and sensitive personal information. |
| Xiaowen and Gavriel (2003) | Consumer's trust in online store sites is influenced by brand names, which can be measured as one of the key factors in dealing with e-commerce transactions. |
| Tan and Sutherland (2004) | The authors treated trust as a multidimensional factor including three elements, namely, interpersonal, institutional, and dispositional trust, with the concern on consumers' trust on e-commerce transactions. |
| Salam et al. (2005) | Trust can be viewed as a complicated social phenomenon reflecting social, behavioural, technological, psychological and organizational interactions among individual and non-human technological agents. |

Table 2.3(ii)

The Selected Prior Researches on Trustworthiness of Web Vendors

| Author(s) | Findings |
|---|---|
| Nam et al. (2006) | The increased on consumers' trust in e-commerce and the benefit e-commerce offers to consumers are two key factors to reduce consumers' concerns on privacy of their sensitive personal information. |
| Carlos and Miguel (2006) | The enlargement of trust affects both the consumers' intentions to purchase, and the effective purchasing behaviour, in terms of frequency of visits, cost and preference, and thus, the level of productivity provided by each consumer. |
| Hann et al. (2007) | Web vendors could provide adequate privacy policies in their online store sites, and their intensions on the collection and distribution of consumers' sensitive personal information in order for obtaining increased value from their consumers. |
| Elena and Miguel (2008) | The findings from a sample of 265 subjects faced with the decision of buying a travel package from an unknown online travel agency showed that association and similarity with a known brand are factors that promote consumers' trust and behavioural intentions. |
| Sonja, et al. (2009) | The findings from two experimental studies of eBay users showed that trustworthiness judgments are influenced by the text comments associated with negative feedback and also by whether a trust violation is perceived as competence-based or morality-based. |
| Kwek, et al. (2010) | A study of 242 undergraduate information technology students from a private university in Malaysia revealed that impulse purchase intention, quality orientation, brand orientation, online trust and prior online purchase experience were positively related to the customer online purchase intention. |

### 2.5.3 Perceived Risk

Considerable numbers of research findings (Malhotra et al., 2004; van der Heijden, 2003; Kimery and McCord, 2002; Jarvenpaa et al., 2000 and Jarvenpaa et al., 1999) have indicated that there was a considerable negative association existed between consumers' trust and perceived risk. Jarvenpaa et al. (2000) stated that consumers' perceived risk related with e-commerce transaction might decrease their perceptions of control and as a result, might negatively affected the consumers' trust in engaging in e-commerce transactions. Pavlou and Gefen (2004) stated that consumers' trust in web vendors facilitated e-commerce transactions by reducing perceived risk. Unlike traditional commerce, e-commerce involves a diversity of risks, such as credit card

information and product performance, that consumers concern (Salisbury, et al., 2001 and Tan, 1999), and hence based on the much of information, consumers are interesting in risk reducing behaviours (Krishnamurthy, 2001 and Hubl and Trifts, 2000). A study found that consumers observed buying offline to be lower risk than buying online and thus more hesitant consumers were less likely to engage in e-commerce transactions (Tan, 1999). Moreover, the author showed a close correlation between online shopping tendency and risk aversion.

Hubl and Trifts (2000) stated that in terms of consumers' decision making to engage in e-commerce transactions, interactive decision supports, for example, recommendations, interface design which assisted consumers to screen available products, and so on, might have greatly attractive properties. According to Krishnamurthy (2001), the numerous information assets, for example, recommendations, brand, and personalized information, perform as guides which make easy for consumers' choices by reducing risk concerns. A study reported that new consumers might prefer to look for the experts' appeals in order to reduce risk in dealing with e-commerce transactions (Tan, 1999).

The studies reported that consumers' risk concerns related to e-commerce transactions might be influenced by several information sources, for example, recommendations, brand, and personalized information (Deighton and Barwise, 2000 and Shankar et al., 2000). A study by Hong (2002) stated that a variety of sources of information, for example, recommendations, brand, and personalized information were generally influenced in eliminating consumers' concerns on risk in dealing with e-commerce transactions. The author also stated that, especially, information source related to the performance of the product could play an important part to reduce consumers' concerns on risk in dealing with online transactions. With the purpose of estimating brand choices, consumers prefer to trust the statement from word-of-mouth compared to business information resources (Iglesias et al., 2001). However, Harrison-Walker (2001) investigated that consumers habitually gave less attention to positive information than to negative information, and thus, more than half of displeased consumers involved in negative word-of-mouth information source.

As more and more information about the online store site is prepared and simply accessible by consumers, consumers' perceived risk is becoming lower to trust in e-commerce transactions (Mitchell, 1999 and Jarvenpaa and Todd, 1997). Accordingly, consumers' perceived risk for a specific brand is decreased due to the positive information about that brand, while consumers' perceived risk for considered brands is increased with the negative information about that brand, and thus, it could probably change the consumers to competitive brands from the considered brand (Nedungadi et al., 2000). Laforet and Li (2005) found that major obstacles to online banking, in China, were the consumers' concerns on risks, traditional cash-carry banking culture and information technological skills. In order to mitigate consumers' perceived risk, building trust between consumers and web vendors has been identified as a significant solution (McKnight et al., 1998).

Unlike offline purchases, online purchases allow web vendors to decrease consumers' perceived risks, such as time, financial, psychological, and performance risks, by offering personalized information to each consumer (Krishnamurthy, 2001 and Dholakia et al., 2000). The studies demonstrated that consumers' perceived risk related to internet banking was mostly influenced by privacy, security, finance, and performance concerns (Aldas et al., 2009; Littler and Melanthiou, 2006 and Yousafzai et al., 2003). Salam et al. (2003) investigated that the increase in economic incentives and institutional trust reduced consumers' perceived risk in dealing with e-commerce transactions. According to Chang et al. (2005), two types of risk, such as, transaction risk and product risk, can be classified in e-commerce literature. According to the authors, transaction risk can be the ambiguity that somewhat unexpected might come out during the e-commerce transaction processing, whereas product risk includes the ambiguity that the purchasing of the product will equal the receiving levels. In addition, the protection of the information provided to web vendors during online transmitting is related to security risk.

On the other hand, Pavlou (2003) stated that privacy risk referred to the possibility of stealing of consumers' sensitive personal information. The author stated that one of the factors which had affected to the slow growth and development of e-commerce in developing countries was consumer distrust on local internet services and products. The risks in e-commerce are identified as requirements risk, resources risk, web

vendor quality risk, legal risk, client server security risk, managerial risk, physical security risk, outsourcing risk, re-engineering risk, and cultural risk (Wat et al., 2005). The authors investigated that security risk was the main concern to engage in e-commerce transactions. The study of 465 employed respondents by Liebermann and Stashevsky (2002) suggested a framework including the factors influencing the perceived risk aspects, especially security and privacy in dealing with e-commerce transactions. The researchers found that distributing consumers' sensitive personal information, online credit card stealing and the usage amount had significant impacts on both current and future online consumers.

The study highlighted that the consumers' concerns on all types of risks, i.e. time, security, performance, and financial risks, and two main kinds of uncertainty which consumers perceived were: some uncertainty about the choices considered and consequences uncertainty (Littler and Melanthiou, 2006). In China, the findings from 432 young consumers indicated that there was a considerable association existed between perceived risk and trust, and both of them were critical in adoption of the internet banking (Anita et al., 2010). In order to place trust in another party's behaviour involves risk, particularly as such a belief involves doubt as the trustor is unable to confirm his/her decision results prior to performance (Doney et al., 2007). Belanger and Carter (2008) integrated trust of the Internet, disposition to trust, perceived risk, and trust of the government in a framework of e-government adoption, and the authors found that citizens were unwillingly to adopt e-government services due to a lack of trust.

A study by Clay et al. (2010) recognized some of the significant findings, i.e. reciprocity increased self-disclosure; positive social influence to use an online community increases online community self-disclosure; privacy risk beliefs decreased self-disclosure, and online community trust increased self-disclosure. With trust, an individual is willingly to transact, involving financial and sensitive personal information, in a risky relationship. Particularly, since the requirement of trust occurs only in a risky relationship, that is, in engaging in e-commerce transactions involving financial and sensitive personal information, the perceptions on consumers' risks might be observed as a root of trust.

In summary, web vendors can use the technique to decrease the concerns on risk issues of their consumers, and hence, increasing consumers' trust to adopt e-commerce. Therefore, in order to increase consumers' trust, web vendors should guarantee to follow security and privacy policies on gathering, storage, distribution, and sharing of the consumers' sensitive personal information, and thus, it will lead to decrease the risk concerns of consumers by trusting in e-commerce adoption.

The selected prior researches on perceived risk related to e-commerce adoption are exhibited in Table 2.4(i) and Table 2.4(ii).

Table 2.4(i)
The Selected Prior Researches on Perceived Risk

| Author(s) | Findings |
|---|---|
| McKnight et al. (1998) | To mitigate consumers' perceived risk, building trust between consumers and web vendors has been identified as significant solution. |
| Mitchell (1999) | As more and more information about the online store site is prepared and simply accessible by consumers, consumers' perceived risk is becoming lower to trust in e-commerce transactions. |
| Jarvenpaa et al. (2000) | Consumers' perceived risk related with e-commerce transaction might decrease their perceptions of control and as a result, might negatively affected the consumers' trust in engaging e-commerce transactions. |
| Nedungadi et al. (2000) | Consumers' perceived risk for a specific brand is decreased due to the positive information about that brand, while consumers' perceived risk for considered brands is increased with the negative information about that brand, and thus, it could probably change the consumers to competitive brands from the considered brand. |
| Krishnamurthy (2001) | The numerous information assets, for example, recommendations, brand, and personalized information, perform as guides which make easy for consumers' choices by reducing risk concerns. |
| Hong (2002) | A variety of sources of information, for example, recommendations, brand, and personalized information are generally influenced in eliminating consumers' concerns on risk in dealing with e-commerce transactions. Especially, information source relates to the performance of the product can play an important part to reduce consumers' concerns on risk in dealing with online transactions. |
| Salam et al. (2003) | The increase in economic incentives and institutional trust reduces consumers' perceived risk in dealing with e-commerce transactions. |
| Pavlou and Gefen (2004) | Consumers' trust in web vendors facilitates e-commerce transactions by reducing perceived risk. |

Table 2.4(ii)

The Selected Prior Researches on Perceived Risk

| Author(s) | Findings |
|---|---|
| Wat et al. (2005) | The risks in e-commerce are identified as requirements risk, resources risk, web vendor quality risk, legal risk, client server security risk, managerial risk, physical security risk, outsourcing risk, re-engineering risk, and cultural risk. The authors investigated that security risk was the main concern to engage in e-commerce transactions. |
| Chang et al. (2005) | Two types of risk, such as, transaction risk and product risk, can be classified in e-commerce literature. Transaction risk can be the ambiguity that somewhat unexpected might come out during the e-commerce transaction processing, whereas product risk includes the ambiguity that the purchasing of the product will equal the receiving levels. In addition, the protection of the information provided to web vendors during online transmitting is related to security risk. |
| Laforet and Li (2005) | Major obstacles to online banking, in China, are the consumers' concerns on risks, traditional cash-carry banking culture and information technological skills. |
| Littler and Melanthiou (2006) | The study highlighted the consumers' concerns on all types of risks, i.e. time, security, performance, and financial risks, and two main kinds of uncertainty which consumers perceived were: some uncertainty about the choices considered and consequences uncertainty. |
| Doney et al. (2007) | In order to place trust in another party's behaviour involves risk, particularly as such a belief involves doubt as the trustor is unable to confirm his/her decision results prior to performance. |
| Belanger and Carter (2008) | The authors integrated trust of the Internet, disposition to trust, perceived risk, and trust of the government in a framework of e-government adoption, and the authors found that citizens were unwillingly to adopt e-government services due to a lack of trust. |
| Aldas et al. (2009) | The study demonstrated that perceived risk in internet banking was mainly determined by security, performance, privacy and finance concerns. |
| Anita et al. (2010) | In China, the findings from 432 young consumers indicated that there was a considerable association existed between perceived risk and trust, and both of them were critical in adoption of the internet banking. |
| Clay et al. (2010) | The study found that reciprocity increased self-disclosure; positive social influence to use an online community increases online community self-disclosure; privacy risk beliefs decreased self-disclosure, and online community trust increased self-disclosure. |

## 2.6 The Internet Security and the Consumer Protection

The advent and emerging information technologies are speedily changing and software are releasing with almost no concern for security by little or no testing. In fact, security is as bad as, or worse than, what we have heard. The general public is still ignorant of the most of the e-commerce security problems. Dealing with today's economy, thousands of consumers' sensitive personal information are exposed on well-known online store sites. The consumers' records could be easily observed and downloaded by any person through standard browsers, without having much knowledge about information technology.

A study by Ahuja et al. (2003) indicated that the concerns on security and privacy issues were the major obstacles to the growth and development of e-commerce. Theses concerns were investigated to be more essential compared to price. According to many security experts, this is because consumers' sensitive personal information are not protected properly on most of the online store sites. Most e-commerce security breaches occur since system administrators do not properly configure and install the information technologies applications and systems. The problem is that the consumers' sensitive personal information are only often secured during transit between consumers and web vendors, and these information are not stored properly on the online store sites' servers, i.e. without using encryption technique. And many security experts believe that the growth of e-commerce will not reach its potential until online store sites strengthen the security by making sure that all consumers' sensitive personal information provided are being securely encrypted by hiring skilled and expertise administrators to organize and uphold software and networks.

The Canadian Working Group on the Consumer and Electronic Commerce outlined the principles of consumer protection on security of payment, privacy, information, personal information, contract formation, redress, liability, consumer awareness, and unsolicited commercial e-mail. Sipior et al. (2004) indicated that online consumers were often motivated to provide sensitive personal information, i.e., their credit card information, name, e-mail address, and postal address, by considering that the information were collected only for intended purpose, i.e., the delivery of their purchased products. On the other hand, when consumers' sensitive personal

information is used for unintended purposes, the privacy violation is particularly occurred.

According to Moores and Dhillon (2003), the three main privacy seals, namely, TRUSTe, WebTrust, and BBBOnline, could essentially enforce the principles of the privacy of information that recipients have agreed to comply with. Up to date cases emphasize the potential for information privacy abuse since only a few commercial Web sites have any sort of privacy statement among the hundreds of thousands of commercial Web sites in existence.

## 2.7 Thefts and Fraud on the Internet and the World Wide Web

These terms; intruder, hacker, or attacker, are used for the individuals who try to find making the use of weaknesses in computer systems and software for the purpose of their own gain. It is essential to understand that every web vendor has full responsibilities to carefully analyze each and every transaction over the Internet. The types of people who exit on the Internet are quite diverse in the physical world in which we live, from scientists to business professionals to children to criminals.

The place we visit on the web can vary from wild to academic to detestable as with the physical world. For these reasons, it is essential that we treat the people we deal with and the places we go on the Internet with caution. Whenever we visit unfamiliar Web sites or sites with which we have had no prior relationship we need to exercise caution. Fraud and theft are made possible on the Internet while consumers willingly trust the web vendors without have had experienced with those web vendors (Ghosh, 2001).

Today, identity theft (fraud) can be described as the greatest rising crime that consumers, web vendors and governments face. It causes for victim consumers, money losses, ruined reputation and leaving with a poor credit rating. Online theft can be defined as getting others' sensitive personal information and utilizing them for the purpose of committing illegal activities without others' knowledge or consent. Online

thieves only need consumers' names, addresses, and date of births to disturb some individuals' lives.

During calendar year 2008, the Federal Trade Commission (FTC) received 1,223,370 Consumer Sentinel complaints. Out of which, 313,982 (26 %) were related to identity theft. The list, contained in the publication "Consumer Sentinel Network Data Book for January-December 2008," revealed that for the ninth year in a row, identity theft was the number one consumer complaint category. The top methods of identity theft reported (in cases where the methods were known) were: credit card fraud, government documents and benefits fraud, employment fraud, phone/utilities fraud, and bank fraud. 65 percent of those who reported identity theft to the FTC did not report the crime to their local law enforcement agencies. Of the identity theft methods reported, credit card fraud complaints and automobile-related complaints had nearly doubled. The report stated that credit card fraud was the most common form of reported identity theft at 20 percent, followed by government documents/benefits fraud at 15 percent, employment fraud at 15 percent, phone or utilities fraud at 13 percent, bank fraud at 11 percent and loan fraud at four percent. Table 2.5 shows the top 20 complaint categories in 2008.

Table 2.5(i)
The Top 20 Complaint Categories in 2008 (the Federal Trade Commission, US)

| Rank | Category | Complaints | % |
|---|---|---|---|
| 1 | Identity Theft | 313,982 | 26 |
| 2 | Third Party and Creditor Debt Collection | 104,642 | 9 |
| 3 | Shop-at-Home and Catalog Sales | 52,615 | 4 |
| 4 | Internet Services | 52,102 | 4 |
| 5 | Foreign Money Offers and Counterfeit Check Scams | 38,505 | 3 |
| 6 | Credit Bureaus, Information Furnishers and Report Users | 34,940 | 3 |
| 7 | Prizes, Sweepstakes and Lotteries | 33,340 | 3 |
| 8 | Television and Electronic Media | 25,930 | 2 |
| 9 | Banks and Lenders | 22,890 | 2 |
| 10 | Telecom Equipment and Mobile Services | 22,387 | 2 |
| 11 | Computer Equipment and Software | 21,442 | 2 |
| 12 | Business Opportunities, Employment Agencies and Work-at-Home | 20,286 | 2 |
| 13 | Internet Auction | 17,294 | 1 |

Table 2.5(ii)

The Top 20 Complaint Categories in 2008 (the Federal Trade Commission, US)

| Rank | Category | Complaints | % |
|---|---|---|---|
| 14 | Advance-Fee Loans and Credit Protection/Repair | 17,263 | 1 |
| 15 | Health Care | 16,275 | 1 |
| 16 | Auto Related Complaints | 14,278 | 1 |
| 17 | Travel, Vacations and Timeshare Plans | 13,200 | 1 |
| 18 | Credit Cards | 13,196 | 1 |
| 19 | Magazines and Buyers Clubs | 10,188 | 1 |
| 20 | Telephone Services | 9,300 | 1 |

The study shows that many of the online deception are due to unreal web vendor created an online store site which looks like a legal store site, as in reality, it is for criminal purposes. Consumers are deceived into giving their credit card numbers for product or services that are never delivered. Another example of fraud that gained notoriety in the Internet security community involves pornography and phone bills. This combination is another case of tried and true scandals that have now penetrated to the Internet, with a twist of technical innovation. Web suffers were unpleasantly surprised with telephone bills in the hundreds and even thousands of dollars that resulted from visiting a pornographic Web site (Bond, 2002).

In electronic transaction, how to catch the theft is the challenge because they can steal in second. Identify theft and misrepresentation are becoming increasingly troublesome. Identify theft can also be defined as the illegitimate gaining of sensitive personal information such as credit card number, name, and so on, in order to deal with criminal acts (Sorbel, 2003). It is the top rising crime in this day and age. The ability to truly know with whom we are dealing with for e-commerce transactions is essential. Thus verification services are essential for the growth and development of e-commerce successfully. Protecting privacy and safeguarding information entrusted to others are also necessary. Online store sites should place sufficient site security, its privacy policy, sufficient encryption, and probably, assurance against online thieves. Therefore, vendors should not place their business over the Internet to engage in transactions involving financial and sensitive personal information, without cautiously considering the control of a theft of consumers' sensitive personal information nowadays.

## 2.8 E-Commerce Security Problems

Many people think that only at the time of the sale, the biggest security risk on the Internet occurs, i.e. when an individual's sensitive personal information is provided to the web vendors through the Internet. In the early days of the e-commerce, individuals were possessed with the belief that online thieves could obtain their sensitive personal information during in transit between consumers and web vendors. Therefore, web vendors focused their security efforts on securing their consumers' sensitive personal information by ensuring that it wasn't sent in the clear by using encryption technique, and it could transfer securely during online transit without being interrupted by unintended parties.

In reality, security breaches mostly occur after the completion of sale, i.e., while customers' sensitive personal information is storing unencrypted web vendors' computing system. There are two ways for someone who wanted to steal a few credit card numbers by hacking into merchant's store. First, somehow the hacker might set out to monitor web vendor's network connections by hopping that web vendor is not using encryption technique that mix up any credit card numbers during transit between web vendor's consumers and his/her online store site. But it does require specialized knowledge and undertaking such a task probably involves a high level of proficiency; it is not beyond the reach of some hackers. All that effort might produce a credit card number or two. Thus this way can be the hard way for some hackers (Heuvelmans, 2000).

Second, the hackers break into web vendor's store site, and then browses around to spot if there is a file that contains customer information, including credit card numbers (Sorbel, 2003). This way, a successful hacker can view and download a file of several thousand consumers' sensitive personal information. Therefore this can be the easy way for hackers. Clearly, the second method produces "better" results. Therefore, securing web vendors' online store sites is much more important than protecting the commercial transactions during transit while engaging in e-commerce transactions.

## 2.9 Significance of the Providing Adequate Internet Security

When the Internet was invented over 30 years ago, it was a collaborative effort between industry, government, and academia. Internet was designed to be an open, borderless medium for communicating and sharing research information. And it was designed to be expandable and to survive natural or artificial disasters by using packet switching technologies. The Internet was not programmed with security features since open sharing of information was the design objectives. In fact, the Internet was not intended for sensitive commercial or government use. Yet, at this day and age, business and government are both deeply devoted to the Internet regardless of its inherent incapability to provide even a bit of security beyond enhanced survivability. Today, both the IT industry and Internet users are playing security catch up (Braithwaite, 2002).

E-commerce applications and Internet technologies go hand in hand. Building security into existing applications is one of the aspects of Microsoft's mission for Internet security. For the purpose of electronic commerce on World Wide Web, it is important that clients authenticate themselves to servers and that servers authenticate themselves to clients. Several techniques have been formulated and spread to ensure security on the Internet. These are: encryption technique, firewalls for the perimeter security, data integrity, and authentication of clients and servers. E-commerce transaction security is crucial and without it, consumers' sensitive personal information will be accessible by unintended parties during transit and then will be misused for criminal activities. Security is required to make sure that unintended third parties cannot eavesdrop on e-commerce transactions, or download or modify data (Microsoft).

Only securing the e-commerce transactions, however, is not enough for all kinds of businesses running on the Internet, and thus, web vendors have to address all types of security, privacy, trust and risk concerns of their consumers' sensitive personal information in order to achieve e-commerce growth. Before engaging in e-commerce transaction, consumers must be willingly to trust the web vendors to provide their sensitive personal information. Emerging security technologies are not enough to protect consumers from web vendors with whom they might choose to do

business though technologies might secure the communication between consumers and web vendors during transit. Kalakota and Whinston (1997) stated that the consumers must be willing to take the additional step and trust the web vendors in order to engage in e-commerce transactions.

Equally, online store sites must take further safety measures to prevent security violations. Web vendors require upholding security of their servers and controlling access to confidential keys and software passwords in order to protect consumers' sensitive personal information. In developing consumers' confidence in electronic commerce, techniques such as private and public-key encryption and digital signatures play a crucial role.

## 2.10 The Need for Trust to Create Secure E-Commerce

Trust can be viewed as a complicated social phenomenon reflecting social, behavioural, technological, psychological and organizational interactions among individual and non-human technological agents (Salam et al., 2005). According to Tang et al. (2003), the followings are three basic forms of trust in trading.

- *Markets pace trust*: The trust that both buyer and seller should have in the markets pace where the transaction will take place.
- *Buyer's trust*: The trust that the buyer has that the expected products will be delivered.
- *Seller's trust*: The trust that the seller has that he or she will be paid for the delivery of products.

The issue of trust is equally essential to both parties involved, i.e. the web vendors should require to authenticate the characteristics of their real consumers, and the consumers need to identify that they are dealing with the legitimate web vendors. Therefore, security can be applied to grant the five important services listed below, which are the basis for e-commerce transactions:

1. *Confidentiality* – consumers' sensitive personal will be accessible only by authorized parties.
2. *User Authentication* – confidence that the involved parties those are engaging in e-commerce transactions are legitimate users.
3. *Server Authentication* – confidence that the information come from original source.
4. *Data Integrity* – confidence that consumers' sensitive personal information has not been altered by unintended users.
5. *Non-repudiation* - the requirements of the entities to a transaction engaged, and later, the transaction cannot be rejected.

A variety of security techniques and processes are used to offer the structure for trusting e-commerce by presenting a number of the above five essential services. However, these listed five services only secure the transactions communications between consumers and web vendors. Therefore, web vendors have to secure their online store sites and computing systems as an extra security requirement (Heuvelmans, 2000). This is because the most security breaches happen while consumers' sensitive personal information are storing at unencrypted web vendor's information systems. A successful hacker can view and download numerous consumers' sensitive personal information easily from unprotected online store sites.

## 2.11 Risks for Online Consumers and Web Vendors

In dealing with e-commerce nowadays, both consumers and web vendors face high level of uncertainties because physical verifications are not possible on digital environment. Everyday, many consumers try to deal with e-commerce transactions, however, majority of them ended up with buying the products from offline store without carrying out the entire e-commerce transactions processes. This is because most of the consumers fear to provide their sensitive personal information to any online store sites and that they do not simply trust most online store sites to deal with commercial transactions involving financial and sensitive personal information. Most

online commercial store sites today are not focusing on building and fostering trust as part of a continuing relationship with their consumers (Salam et al., 2003).

Consumer risks having their sensitive personal information stolen by hacker, and then the theft can use their credit card number at will until credit limit is reached. Online store site may be an unreal and then consumers just lost the money. The consumer's sensitive personal information might be used for the purpose of spam, blackmail or profiling against the consumer. Web vendors could be observable consumer's purchasing habits and increase product price to meet the consumer's cost ceiling. Others, to gather consumer's sensitive personal information may control consumer's browser. The consumer's machine might be taken by rogue programmers through the browser (Ghosh, 2001). Therefore,

- How can the consumer be sure that the online store site is owned and operated by a legitimate web vendor?
- How does the consumer know that the online store's pages and forms do not contain some dangerous or malicious content or code?
- How does the consumer know that the web vendor will not share their sensitive personal information provided to other parties?

Risks for web vendor included consumer might find link broken and purchase from other competitors; consumers might be competitors, inspecting for price comparisons, and consumers' sensitive personal information might be stolen from their online store sites. Hacker might view and download all consumers' sensitive personal information, opening liabilities to web vendors, might order many fake purchases, might put in reverse orders, increasing consumers' credit card balances, and might send unreal information to consumers. Therefore,

- How does the web vendor know the consumer will not try to break into the web server or modify the pages and content at the online store site?
- How does the web vendor know that the consumer will not attempt to interrupt the web server so that it is not accessible to other legitimate consumers?

Risks for both online consumer and web vendor included:

- How do they know that the network system connection is free from snooping by unintended third party?
- How do they know that the information sent back and forth between the web vendor and consumer's browser has not been transformed during transit?

## 2.12 Risks for E-Commerce over the Internet

Nowadays, for the smooth performance of the business functions, many vendors are seriously depending on information technologies. When these systems are either limited as to their interaction with outsiders or inaccessible from the outside world, each system is still under control of its organization. However, when these systems are used for business purposes over the Internet and World Wide Web, organizations' control over the system becoming less and less since they need to depend more and more on technology for e-commerce to be successful and growth.

By using information technology, criminals' risk of being caught is considerably reduced as no physical existence is needed and verification is difficult to gather, and also the lack of legislation across the borders between countries. Although many organizations acknowledge that security is of the utmost importance, securing the Internet is beyond the control of information security professional experts, at present. Even though with the development and design of secure information technologies have been prepared as good progress, there is still a need for a information security professional expert to apply and uphold theses technologies (Labuschagne and Eloff, 2000).

For all practical purposes, nobody is responsible for any security breaches that may arise over the Internet, as the Internet is non-ownership and have to use it at our own risk label. Therefore, those organizations that offering goods and services in the electronic marketplace need to be ready to take complete responsibilities for risks incurred on the Internet in dealing with e-commerce. The only way to address effectively these risks is to handle them accurately.

In addition, technology risks could be incurred for the Internet subscribers beside business risks. The Internet is ever changing technology and it constitutes a very dynamic environment. Organizations have almost no control over happening on the Internet outside their perimeters since the nature of the Internet makes it so complicated to secure. Therefore, at any point in time, it is not possible to believe that the e-commerce activities of any one organization are secure.

In addition, there are many diverse types of security risks that can affect online businesses. Some of them are:

*Malicious Software:* Viruses are malicious programs that can modify files, steal passwords, damage or delete data on our computer, and even transfer files from our computer to other computers on the Internet, oftenly without our knowledge. All computers, from mainframes to personal digital assistants (PDA) and cell phones, are intimidated by the virus phenomenon. An example is the famous Love Bug virus that paralyzed hundreds of thousands of computers around the world in 2000. The virus caused an estimated $ 15 billion worth of damage and forced thousands of organizations to shut down their e-mail systems (Jim Carroll and Rick Broadhead, 2001). We can infect our computer with a virus by opening an e-mail or computer file that is already infected with the virus.

Worm is malicious software application designed to propagate through a Network rather than through a single computer. It can manipulate flaw in the network transport such as mail, ports and so on. Multitasking computers using open network standards are especially vulnerable to worms. A Trojan horse is malicious software program hidden in other software that is being distributed as a useful program. The Trojan horse may be a virus or worm, or it may be surveillance software, such as a *cookie*, which communicates information back to an executor. A Trojan horse will not execute unless the user runs the software in which it is hidden.

Time Bomb is a virus, worm, or other malicious software program code designed to trigger at a certain date and time. Enough lag time is usually allowed, following introduction of the bomb, to ensure widespread distribution of the code throughout the organization before the activation date and time. *Logic Bomb* is also a virus, worm, or other malicious software program code designed to trigger under

certain conditions. *Rabbit* is a worm designed to duplicate to the point of exhausting computer system resources by consuming all processor cycles, disk space, or network resources (Braithwaite, 2002).

By installing and frequently updating on virus protection software on our computer from well-known companies such as McAfee and Symantec are the greatest way to defend us against viruses and other malicious program codes. Both companies provide extensive information on their Web sites to help us learn about viruses and guard against them. We should also ensure that all of the information on our computer is backed up in the event that a virus wipes out some or all of the files on our hard drive. Once vendors are being running their online store sites, they have to think of all the important data that they will have on their computer systems such as consumers' records, order history information, credit card numbers, product data, and more. It would be a complete disaster if web vendors were to lose all of the information due to malicious software.

*Snooping Attacks:* When somebody listening in particular web vendor's online store site and tries to gain consumers' sensitive personal information during transit is called snooping attack. *Eavesdropping* means intercepting and reading messages intended for other principals (Ghosh, 1998). Snooping is also performed by trusted but curious system users. Indicator includes unusual system access activity during off-hours. We can minimize our vulnerability to a snooping attack by encrypting the information so that it is scrambled, making it unintelligible to an eavesdropper. Although the risk of a snooper is slim, this is probably the one security issue that online shoppers are most terrified of. The most accepted technique to scramble a consumer's credit card number is to use encryption technique called SSL (Secure Sockets Layer) (Ford and Baum, 2001). Most online storefront products use SSL to ensure that consumers can transmit their sensitive personal information to web vendor's online store site safely and securely.

*Web Site Break-Ins:* A break-in occurs when an individual drives their way into online store site in order to get access to consumers' sensitive personal information, i.e., cardholders' data, passwords, billing records and so on. By using firewalls and other sophisticated security measures to limit who can gain access to a

Web site or a computer network, this type of risk can be reduced (Ford and Baum, 2001).

*Security Leaks:* When private information is able to be seen on an online store site while it should not be, a security leak occurs. This usually happens because someone has not properly secured the Web site. Additionally, security leaks can happen while illegal access by employee from same organization, or by someone at an Internet service provider (Jim and Rick, 2001).

*Intentional Destruction of Data:* Sometimes, people break into Web sites with the sole intention of vandalizing the site in some manners. In order to make a public statement of some kind usually the culprits alter the images or graphics on the Web and add their own (Jim and Rick, 2001). If web vendor's store site is not properly protected against unauthorized access, web vendor might find himself in a very embarrassing, and potentially costly, situation.

*Accidental Loss of Data:* Web vendor's could also lose consumers' sensitive personal information or even whole online store site due to human error even though we want to protect our online store in the event of a computer crash, power failure, flood, other disaster at the location of our Inter service provider, storefront service provider, or Web hosting company. For example, some commands on UNIX operating systems are so powerful that a single accidental command could wipe out everything (Jim and Rick, 2001). These risks are best avoided by controlling access to web vendors' computing systems as well as by regularly backups of their online store sites.

*Denial of Service Attacks:* A denial of service attack occurs when an individual intentionally blocking access to web vendor's online store site by bombarding the web vendor's computing systems by means of a stream of information requests. There have been many high-profile cases of web sites being shut down, or made inaccessible or intolerably slow, as the result of what is called a denial-of service attack. The information requests ultimately overpower web vendor's computing systems, making it to close down. Such an attack exploits a problem within the operating system software or other software upon which a Web site or online store is based. The much-publicized attacks in 2000 that temporarily shut down several Web sites, including

Yahoo!, Amazon.com, and eBay were denial-of service attacks (Jim and Rick, 2001). By a displeased consumer, electronic joy rider, or a competitor, web vendor's online store could be subject to a denial of service attack. Denial of service attack can occur because of known bugs in particular software programs, and thus are most excellent avoided by assuring that the web vendors use up to date software for their online store sites, together with latest version of operating system and web server.

*Unauthorized Modification and Integrity Attacks:* Someone probably has the capability to change the prices or product information if that person can break into the online store (Ford and Baum, 2001). This could have an embarrassing or indeed damaging effect on business, particularly if customers make purchases in our online store based on the incorrect information.

*Domain Name Hijacking:* Domain name hijacking occurs when a regular person or a competitor pays for a domain that is very similar to your own. It can occur by winning your domain name and changing it slightly. It happens when someone, by forging your identity or through other means, gains unauthorized access to the central registry database that stores the routing information for your domain name. Unlike the other types of security risks, there is little that you can do to prevent this type of event from occurring. Security for Internet domain names rests with the various domain name registries that allocate domain names to individuals and businesses on the Internet.

*Cyber Extortion:* Cyber extortion is a growing and costly type of criminal activity (Bednarski, 2004). Cyber-extortion happens when a hacker or criminal breaks into the Web site and promises to destroy data, steal consumers' sensitive personal information, set up a denial of service attack, or commit some other act unless a ransom is paid. This has happened to several firms with Web sites. In one case, an online retailer's web site was broken into and customer records were accessed. The hacker threatened to publish thousands of customer credit card numbers unless $100,000 was paid. The company refused, and the hacker proceeded to post thousands of customer names, addresses, and credit card numbers on the Internet (Jim and Rick, 2001). This type of blackmail is an unfortunate reality of doing business on the Internet.

## 2.13 Incident Statistics in Malaysia

When a company begins to offer products or services over the Web, the threat of hacker activity against a target is increased. Table 2.6 shows the Incident Statistics in Malaysia at 2009, adapted from National ICT Security & Emergency Response Centre (NISER).

Table 2.6
Incident Statistics in Malaysia at 2009

| | Jan | Feb | Mar | Apr | May | Jun | Jul | Aug | Sep | Oct | Nov | Dec |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Drones Report | 4 | 3 | 3 | 11 | 8 | 8 | 3 | 9 | 9 | 9 | 16 | 9 |
| Denial of Service | 2 | 0 | 0 | 6 | 6 | 2 | 7 | 1 | 2 | 1 | 1 | 0 |
| Fraud and Forgery | 60 | 86 | 69 | 43 | 73 | 71 | 96 | 108 | 98 | 108 | 96 | 114 |
| Vulnerability Probing | 19 | 6 | 10 | 22 | 17 | 18 | 22 | 16 | 24 | 4 | 15 | 9 |
| Harassment | 16 | 23 | 7 | 17 | 10 | 17 | 22 | 16 | 10 | 13 | 15 | 8 |
| Indecent Content | 2 | 1 | 0 | 1 | 2 | 3 | 3 | 0 | 3 | 0 | 0 | 2 |
| Malicious code | 12 | 23 | 18 | 24 | 19 | 10 | 26 | 16 | 37 | 40 | 42 | 16 |
| System intrusion | 49 | 41 | 220 | 146 | 168 | 209 | 207 | 152 | 170 | 120 | 165 | 119 |
| TOTAL | 164 | 183 | 327 | 270 | 303 | 338 | 386 | 318 | 353 | 295 | 350 | 277 |

All types of online security risks are serious, though DoS attacks can compromise not only one user or Web site, but also an entire network. Even the Internet has been affected by DoS attacks. Some operating systems are more secure than others with regard to some possible attacks. In fact, injuries from hackers are not usually made public because of the potential in negative publicity. Hackers are, sadly, as traditional as e-mail on the Internet. According to Goralski and Waclawski (1999), hackers work with four major methods namely denial-of-service (DoS) attacks, Brute-force password blitz, social engineering, and passive listening.

A study investigated that in large businesses, 48% of the most horrible incidents were caused by internal employees, however, only 32% of the most horrible incidents were caused by internal employees in small businesses (The Information Security Breaches Survey 2002). Another kind of the most horrible security incidents are virus infections. Virus infections are also high incidences and more intentionally target attacks. People constantly introduce new computer viruses that may damage data or be disable the systems. Therefore, any breach of security is serious, not only

due to the direct damage it can make to our reputation and finances, but also due to the liabilities that it can set us open to. Figure 2.7 shows the comparison between Incident Statistics in Malaysia at 2005 and 2006.

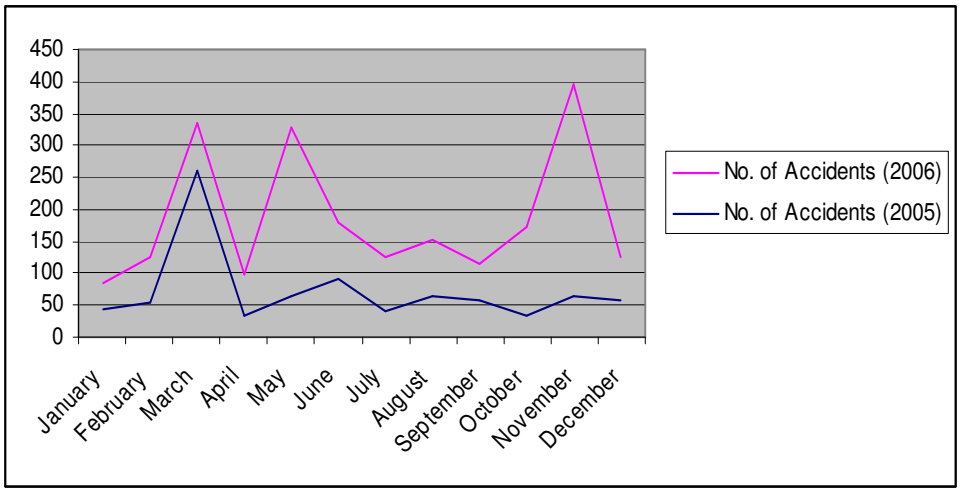



Figure 2.7. Incident Statistics in Malaysia at 2005 and 2006 (NISER).

## 2.14 Threats to E-Commerce and Protection of Online Threats

The enormous increase potential of e-commerce is displeased by legal concerns related to the security of online transaction processing systems. The major concern for both consumers and web vendors in dealing with e-commerce transactions is the possible loss of financial and privacy because of violations in the security of market transactions and business computing systems. The confidence to trust in e-commerce transaction can be taken away by a particular exposed security violation, and not only harm the web vendor's reputation, but also affect the entire e-commerce business.

According to Ford and Baum (2001), e-commerce could be affected by many different threats, such as, breach in computing systems, violations of authorities, and many more. In order to defend against these risks, secure information technologies provide a variety of safeguards, such as confidentiality, access control, authentication, integrity, and non-repudiation services.

*Consumer account authentication:* Digital signatures and digital certificates ensure consumer account authentication by providing a method that connects a consumer to an exact account number. Secure Electronic Transaction (SET) assigns a third party certificate authority to validate the consumer and web vendor. Therefore, web vendor have to confirm for a legitimate consumer holding legally binding account number.

*Web Vendor authentication:* Web vendor authorized certificates and Digital signatures are used to authenticate for a legitimate web vendor. Secure Electronic Transaction (SET) provides a method for consumers to verify that a particular web vendor has a connection with financial organizations that allows that web vendor to accept bank card payments.

*Confidentiality of information:* To facilitate and encourage financial transactions on the web, it is essential for web vendors and banks to promise the consumers that their sensitive personal information is secure and accessible only by the expected recipients. The Secure Socket Layer (SSL) specifications provide confidentiality by using encryption technique. Therefore, consumers' sensitive personal information have to be saved and secured during transit without altered by unintended parties in dealing with e-commerce transactions.

*Integrity of information:* Electronic payment information provided by consumers to web vendors contains consumers' sensitive personal information, order and delivery information, and instructions for payment. The e-commerce transaction will not be able to process precisely, if any part is altered during transit. The Secure Socket Layer (SSL) offers the way to make sure that all the contents of information received match the contents of information transferred. SET ensures that the contents of the information are not altered during transit between consumer and web vendor. Digital signatures are used to ensure the integrity of information.

*Non-repudiation*: the requirements of the entities to a transaction engaged, and later, the transaction cannot be rejected. Secure Electronic Transaction (SET) specifications provide non-repudiation.

## 2.15 Consequences of Inadequate Data Security

Most importantly, web vendors reveal themselves and their consumers to incredible risks by not sufficiently protecting their consumers' financial and other sensitive personal information such as names, addresses and telephone numbers. If online thieves are able to get access to a web vendor credit card data, some or all of the web vendor's consumers can be victims of online fraud (Ford and Baum, 2001).

Fearing that their financial and sensitive personal information would not be secured, consumers might stay away from insecure online store, resulting in a sharp drop in business. The negative media attention that often results from a hacker attack can trouble a web vendor for years, not to mention the devastating impact on the web vendor's reputation. For example, consider what happened to Western Union following the hacker attack. The story was immediately picked up by the news media and reported widely. The negative publicity from this event harmed Western union's reputation and credibility, making many consumers think twice about using the company's Web site (Jim and Rick, 2001). An April 2003 survey (Electronic Payments, 2003) found that 70% of U.S consumers are concerned about security. The other factors that were stopping U.S consumers from dealing with e-commerce transactions online were: hassle to provide consumers' sensitive personal information (about 9%), didn't have a credit card (about 7%), didn't wish to pay interest charges (about 6%), small purchase value (about 4%), and personal limit exceeded (about 4%).

Inadequate security on the online store site could also result in the revocation of the vendors' accounts. Every time a fraudulent transaction occurs on e-commerce store site, the web vendor will probably receive a chargeback for the purchase once the real cardholder discovers the fraudulent activity. If the web vendors begin to get a lot of charge-backs because of online deception, well-known financial institutions, i.e. American Express, MasterCard, and Visa, reserve the right to cancel the web vendor status so that the web vendor can not accept credit cards anymore. Clearly, this could be devastating to online business. More serious might be the fact that the merchant cannot fund the charge-back. This is a more likely risk to legitimate merchants who have a weak security (Brancheau and Nansi, 2001).

But those are not the only consequences that the web vendors may face. Credit card companies such as Visa are stepping up their enforcement of Internet security and creating compulsory security rules for the web vendors and their service providers. The web vendors and their service providers who fail to obey can face stiff fines, be subject to a cap on the dollar amount of sales they can process through their online stores, or lose their web vendors status altogether. In order to avoid these penalties, the web vendors should check with their account provider or acquiring financial institution to obtain the most current security rules for each of the credit cards the web vendor accept on the Internet (Ford and Baum, 2001). For example, Visa USA has created a Cardholder Information Security Program that includes minimum-security requirements that must be followed by any organization that processes, stores, or has access to credit card data from Internet transactions. Therefore, the web vendors, the organization that hosts online store site, or any other service providers that might be involved with online store site must follow to include the minimum-security requirements for online stores to be successful.

## 2.16 Online Secure Payments for Successful E-Commerce

With the purpose of securely participating in e-commerce, it is important to realize what security attributes are and are not provided by a given protocol. IPv4 (Internet Protocol Version 4) was employed as the primary protocol for the Internet and it has served its purpose worthily for nearly 30 years. Nowadays, IPv6 (Internet Protocol Version 6) is being implemented as a significant technology to offer better services for existing technologies and applications by providing better security than IPv4 for applications and networks as well as to meet increasing demands of new devices. It is important for web vendors and consumers to intelligently choose the right protocol for their needs. Before launching into the e-commerce payment systems, one must recognize existing protocols widely used in securing web-based transactions. The Secure Sockets Layer (SSL) makes possible for secure communication between consumers and web vendors in dealing with e-commerce transactions nowadays (Ghosh, 2001).

Since e-commerce transactions risks can generate a major barrier to the acceptance of marketplace, its control and management are important for web vendors' reputation and the encouragement of consumers' trust in addition to operational effectiveness (Liao and Cheung, 2003). In order to gain the consumer to trust in e-commerce transactions, it must be a secure and safe online environment. The concept of privacy lifts up sensitive social and political issues (Sithamparam, 2001). The aim of e-commerce is to build up a set of payment techniques that will be able to use broadly by consumers and broadly accepted by web vendors and financial institutions in dealing with e-commerce transactions. Payment is one of the key features of an e-commerce transaction. Electronic payment can be defined as monetary exchanges that take place electronically between consumers and web vendors. It is an important part of e-commerce transaction. The need to decrease costs is one major reason for the increase in electronic payments. Consumer electronic payment systems are growing speedily, but the opportunities are barely tapped.

For e-commerce business today, many protocols are currently employed for online payment methods in dealing with e-commerce transactions. However, SSL and SET are used for online payments among several Internet-based payment methods, facilitated by service providers. Market acceptance and user confidence in the Secure Sockets Layer (SSL) protocol, formulated by Netscape, is extremely high and widely deployed today on the Internet for e-commerce business. The Secure Electronic Transaction (SET) specifications, developed by Visa and MasterCard and several other companies, support online payments as a part of e-commerce transactions. The goal of SET is to provide a more secure environment than that offers through traditional SSL-protected bankcard payments on the Internet.

## 2.17 Chapter Summary

The advent of technological capabilities and the Internet have created e-commerce a major element in today economy. However, consumers' concerns on security, privacy, trustworthiness of web vendors, and risk issues have weaken the growth and development of e-commerce successfully. The review of the literature has revealed

that web-based businesses always have required to gather their consumers' sensitive personal information. By using the advent of technological capabilities, web vendors can easily collect, store, analyze and even misused consumers' sensitive personal information than ever before.

Many researches have carried out to achieve a better understanding of the consumers' perceptions related to security and privacy issues. Some studies focused on the processes web-based organizations use to gather and distribute consumers' sensitive personal information whereas others focused on consumers' attitudes toward e-commerce adoption and their personalities in dealing with e-commerce transactions. In general, all the researches have pointed out a clear image of consumers' concerns on security and privacy issues, trustworthiness of web vendors and risk concerns in order to trust in e-commerce transactions. Many researchers concluded that in order achieve the growth and development of e-commerce, web-based organizations needed to manage consumers' concerns adequately.

Building trust between consumers and web vendors in e-commerce and offering beneficial incentives in dealing with e-commerce have been recognized as some revenues to lessen the consumers' security, privacy and risk concerns, and thus, it will lead to adopt e-commerce transactions. Some web-based organizations have offered economic incentives as a means of reducing consumers' concerns on security, privacy and risk for providing their sensitive personal information to web vendors. The present study has addressed by identifying the influential factors for consumers' trust in e-commerce adoption. The literature review confirmed that the significance of this study inhabited in providing web-based businesses with the means to lessen their consumers' concerns and, thus, contributing to the growth and development of e-commerce.

The detail of the research framework, the chosen research method, target population, sampling, the development, design and construction of the questionnaire, reliability and validity examining of the collected data, and the suitability of the statistical measures used (SSPS 12.0 and AMOS 18.0) will be explained in the next chapter.

# CHAPTER 3

# RESEARCH FRAMEWORK, METHODS AND APPROACH

## 3.1 Introduction

In this chapter, the detailed information of the framework on which this research is based, and also an illustration and explanation of the conceptual research model adopted in line with the literature review is presented. The research model is designed to study how consumers' perceptions about security and privacy, trustworthiness of web vendors, and their risk perceptions affect their intentions to trust in e-commerce transactions, and thus, it will lead to their confidence to adopt e-commerce. The chosen research method, the target population, the sampling procedure, and the required sample size are presented. The survey's reliability and validity are discussed. And the methods of data collection and data analysis procedures are presented.

## 3.2 Proposed Research Model

With the explosion of information technology, information system researchers have contributed extensively to the development of theories that foresee the recognition of Information Technology. According to Horton et al. (2001), Technology Acceptance Model (TAM) becomes one of the mainly applicable and useful models for computer use and has been validated through a number of technologies.

A study of Anandarajan et al. (2000) acknowledged that the basic of the Technology Acceptance Model (TAM) lies in a number of psychological theories. The Theory of Reasoned Action (TRA) had been widely used in IS research and have also been applied areas relating to Information Technology acceptance as well as in

electronic commerce research. The Theory of Reason Action is a behavioral theory which states that reasoning flows from belief and evaluation to the development of attitude towards performing a behavior. The Theory of Planned Behavior (TPB) (Ajzen, 1991) has the additional component of perceived behavioral control as the determinant of intention. Before consumers are being influenced by the usability features of an online store site, they have to cross security and privacy concerns as the first obstacle so as to come to a decision to participate in e-commerce activities. Therefore, this study prefers the behavioral model over Technology Acceptance Model as the background for the proposed model because the behavioral model is best suited in understanding consumers' buying behavior.

The factors considered to be associating consumers' confidence to adopt e-commerce are categorized into four main groups: consumers' attitude towards secure online transaction processing systems, privacy of consumers' sensitive personal information, trustworthiness of web vendors, and consumers' perceived risk in e-commerce transactions.

### 3.2.1 Perceived Information Security

Attitude towards the online transaction process is conceptualized to reflect a consumer's belief or perception of the online transaction process, and the attitude relates to the process is based on the consequences the processing system is perceived to have on the consumer in the course of the transaction. The concerns on security refer to the degree to which one believes that his/her sensitive personal information will be transmitted securely over the Internet and will be accessible only by intended recipient. The items includes are adapted from Salisbury at al. (2001). There are five items that are conceptualized to measure the attitude related to transaction processing system in this model, namely, "feel safe providing info over web", "accessible only by intended recipient", "information is not altered in transit", "not hesitate to purchase", and "adequate control to ensure security".

### 3.2.2 Perceived Information Privacy

In the context of e-commerce, an individual privacy concerns are influenced by his/her perceptions. The 6 items includes for perceived privacy are adapted from Malhotra et al. (2004). The items includes are “information will not be misused”, “control over how info will be used”, “later verify information”, “companies will not reveal information”, “effective mechanism to address violation”, and “adequate control to ensure privacy”.

### 3.2.3 Trustworthiness of Web Vendors

Since consumers disclose their sensitive personal information, i.e., name, credit card information, and addresses, when they plan to engage in e-commerce transactions, they are exposed to the acts of web vendors. Consumers have only limited control to observe the acts of the web vendors concerning the misuse of their sensitive personal information, and thus, consumers are unwillingly to disclose their sensitive personal information to web vendors in order to deal with e-commerce transactions. The items measuring trustworthiness of web vendors are adapted from Bhattacherjee (2002). The items includes in this study are “online companies will act with high business standards”, “companies have the skills and expertise”, “companies are dependable”, “companies do not have ill intensions about consumers” and “companies are trustworthy”.

### 3.2.4 Perceived Risk

Perceived risk refers to the ambiguity the consumers believe while they decide to buy from web vendors involving financial and sensitive personal information. The items measures for risk perceptions in this study are adapted from Malhotra et al. (2004) and Jarvenpaa et al (1999). The three items includes in this study regarding risk concerns are “providing credit card information over the web is unsafe”, “risky to give personal information to web vendors” and “too much uncertainty associated with providing personal information”.

Salam et al. (2003) indicated that the increase in economic incentives and institutional trust reduced consumers' perceived risk in e-commerce transactions. The items measures for economic incentives and institutional trust are adapted from Salam et al. (2003). The items includes in this study regarding economic incentives are "providing information is not matter for lower price" and "providing information is not matter for higher quality" and items relates to institutional trust are "trust to open financial account with a bank" and "trust to open financial account with a major credit card company".

### 3.2.5 Consumers' Trust

Consumers' trust refers to the consumers' decisions to deal with e-commerce transactions and their willingness to continue purchasing over online environment involving financial and sensitive personal information. Consumers' trust measures in this study are based on Ahmed et al. (2007). The items includes are "confidence for complex and advanced method" and "confidence for all necessary guarantees".

The research model, as shown in figure 3.1, is proposed to examine consumers' attitudes towards secure online transaction processing system, privacy of consumer's sensitive personal information, trust and reliability of web vendors, and consumers' perceived risk related to e-commerce adoption. The model is built based on the combination of the theoretical and empirical studies.

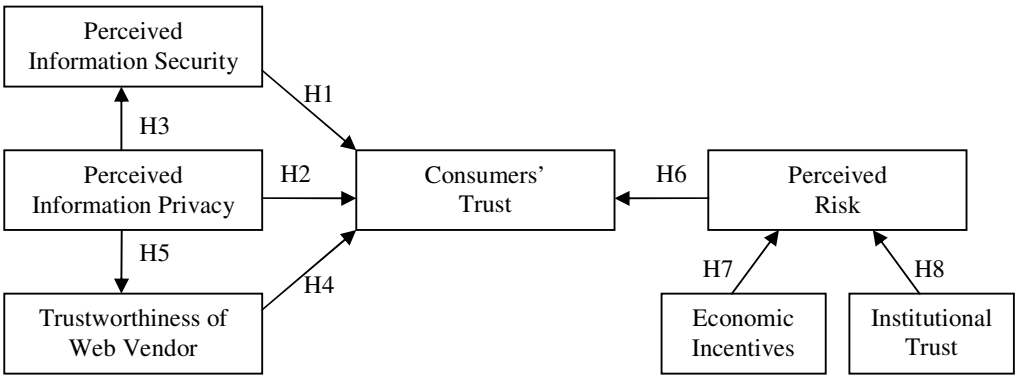



Figure 3.1. The Research Model.

Specifically, the following hypotheses are to be tested in this study:

**H1:** A consumer's perceived security of online transaction positively influences his/her trust in online transaction.

**H2:** A consumer's perceived privacy of online transaction positively influences his/her trust in online transaction.

**H3:** A consumer's perceived privacy of online transaction positively influences perceived security of online transaction.

**H4:** The trustworthiness of web vendor positively influences a consumer's trust in online transaction.

**H5:** A consumer's perceived privacy of online transaction positively influences the trustworthiness of web vendor of online transaction.

**H6:** A consumer's perceived risk in online transaction positively influences his/her trust in online transaction.

**H7:** The increase in economic incentives reduces consumers' perceived risk in online transaction.

**H8:** The increase in institutional trust reduces consumers' perceived risk in online transaction.

### 3.3 The Chosen Research Method

The Information System researchers now have a wide selection of research methods or designs from which they can choose the most appropriate one to solve their research problems. In recent years, the question of which research method or design is more appropriate to the systems has been in an issue of concern. It is often argued that there is no one best research design or method over another and hence, clearly, the most important aspect to be considered before applying a certain research method is to be aware of its benefits and pitfalls. According to Sproull (1995), the type of

research method shall be chosen based on the type of information required, the availability of resources, the level of control the academician has over the selection and assignment of subjects, and the ability to manipulate the variables of interest.

Businesses of all sizes increasingly rely on the information from surveys to discover how to better satisfy their consumers. Survey method has been mainly adopted in this study since the purpose of the research, the availability of resources, the type of information required and the location of the subjects were the factors that contributed to the choice.

One of the unique factors of survey research methods is to the principal need to collect raw data from large sample sizes of people. In this method, individuals are selected and asked questions and their responses are documented in a precise and structured manner. Nowadays, the advent information technologies allow researchers to create numerous survey research methods.

When choosing a survey research method, researchers have to consider several factors such as quality requirement of the data, completion time frame, budget of available resources, difficulty of the task, amount of information needed, degree of survey participation and many more.

The questionnaire is the preferred tool for many researchers, and it can offer an effective and cheap way of gathering collected data in a manageable and structured form. According to Weiers (2002), the choice of data collection method is influenced by the availability of resources and the suitability of the method to generate the required data.

### 3.4 Questionnaire Construction

Survey research is normally viewed as relating the asking of questions, however, an assessment of a usual survey will most likely expose as many statements as questions. The ultimate goal of most researchers is arranging the survey questions in a way that will motivate respondents to read and respond to the question. In survey research,

both statements and questions can be utilized valuably. Applying both statements and questions in a particular questionnaire contributes more tractability in the items design and also the more interesting questionnaire can be made.

The partitioning of questions into sections according to the similarities and relevancy of the question to the particular section is the most common structure of the questionnaire used among the researchers. The questionnaire for this study is divided into three different sections. Section one contained the questions designed to gather information related to participants' background information. In this section, questions composed information related to respondents' gender, age, academic qualifications, and primary occupation. Nominal measurement is used to measure the variables in this section.

Section two contained the questions dealing with some of the variables related to e-commerce purchases and e-commerce adoption. In this section, questions collected information related to the Internet usage frequency, online purchases frequency, respondents' intentions to keep on with online purchasing, and consumers' intentions to purchase online in near future. Ordinal measurement is used to measure the variables in this section.

Section three contained the questions dealing with some of the variables related to influential factors affecting consumers' concerns on security, privacy, trustworthiness of web vendors and risk issues in dealing with e-commerce transactions. In this section, questions collected information related to attitude towards secure e-commerce transaction processing system, attitude towards privacy of consumers' sensitive personal information, attitude towards trustworthiness of web vendors, and consumers' perceptions on risk in dealing with e-commerce transactions. Interval measurement is used to assess the variables in this section. In this section, Likert scales with endpoints ranging from 1 (strongly disagree) to 5 (strongly agree) is used to measure all of the variables. The questionnaire sample is exhibited in Appendix A.

### 3.5 Refinement of the Questionnaire

The aim of the pre-test and pilot testing is to find problems in the questionnaire and to find the need for further refinement of the questionnaire before sending the final copy to the respondents. The problems could be poor wording of questions and/or incomplete directions that are difficult to understand. There are problems that will always require pre testing the questionnaire before sending to the respondents. Therefore, the completion of questionnaire design does not necessarily mean that the questionnaire can directly be sent to the respondents. In order to assess the need for further refinement of the questionnaire, pilot testing need to be done after conducting pre testing, to modify the questions before sending them out since they cannot be modified once it is sent to the respondents.

#### 3.5.1 Pre and Pilot Testing

According to Shanks et al. (2003), a survey study is valid if it is complete, accurate, non-redundant, and conflict-free. After completing the design of the questionnaire, it is pre tested with ten of research colleagues. Seven males and three female students comprising of six Ph.D students, and four Master students are participated for the pre-test to check for the clarity and wording of the questions. From the pre-test, it is found that two questions needed to be excluded since those questions were not related with the study, and also a few questionnaires needed to be rephrased. After completing the necessary modifications and changes, the redesigned questionnaire is printed for pilot testing. Leedy and Ormrod (2005) stated that the major elements of reliability in the instrument of a survey are stability and consistency. Pilot testing is undertaken in order to obtain a more clear and clarified questionnaire. Pilot testing is conducted on the basic of convenience by distributing to 25 master and doctoral students from different departments of the Universiti Teknologi PETRONAS (UTP) for comprehensiveness, clarity and appropriateness. From the pilot testing, an open-ended question is needed to convert into Likert scales. After modification, the questionnaire is adopted as the final version to be sent to the target respondents for this study.

### 3.6 The Population and Sampling

An important task for a survey researcher is to carefully define the population of interest before collecting the sample. In general, population is a collection of elements about which the researcher wishes to make an inference. Most of the survey research involves the selection of a sample from a population because it is difficult and expensive to study the entire population. According to Sproull (1995), population is all groups of a determined category of elements, for example, objects, events or people. In this study, the population of interest comprises consumers residing or working within Malaysia, and the desired characteristics for the population of interest include all individuals who might or might not have used the Internet for purchases.

For the reason that the setting under this study is e-commerce and consumers' intentions to transact in e-commerce must need to use the Internet, the target population of this study is Internet savvy students and general public. The present study will focus on both Internet savvy students who had not yet experienced with e-commerce transactions as well as Internet savvy general public who had experienced in dealing with e-commerce transactions. This is because Internet savvy students who had not yet experienced with e-commerce transactions could concern more on the security and privacy of their sensitive personal information in order to engage in e-commerce transaction compared to Internet savvy general public who had experienced in dealing with e-commerce transactions.

Choosing the most appropriate sample from the population is necessary for making inferences about the population. Inferences about a population are made based on the information contained in the sample chosen from that population. The procedure for selecting a representative sample from a population of interest is known as sample design (Wilkinson and Birmingham, 2003). Moreover, there is simply no directory of all the Internet users, and their time and level of usage are not being tracked. A sample had to be chosen that most corresponded to the entire Malaysian population for the intentions of this study because studying the whole Malaysian population of Internet savvy students and general public is not viable due to the existence of the millions of Internet savvy students and general public in Malaysia.

Since it is impossible to get the list of all the Malaysian Internet users, the defining and identifying the population of the all the Malaysian Internet users became complicated. Heckathorn (2007) stated that sampling the members of the population became difficulty in the study because it was hard to define and identify. Thus, many standard probability sampling procedures, such as random sampling, proportional stratified sampling, cluster sampling, and systematic sampling, could not be used in this study. For that reason, this study adopted non-probability sampling method. According to Creswell (2007), non-probability saves time, effort, money and also convenient, and thus, it is often a useful means to get to the respondents.

According to Hair et al. (2000), convenience sampling is mostly used in exploratory research. Convenience sampling techniques are considered to be suitable for obtaining data quickly and economically. Seeing as the aim of this study was to obtain consumers' concerns on security, privacy, trustworthiness of web vendors and risk issues related to e-commerce transactions from a wide range of educational backgrounds and age groups, Internet users' students and general public are participated in this study. Since this study is exploratory by nature and the data is required from a sample in a large population, students as well as general public within the Malaysia are chosen as the respondents of this study.

### 3.7 Administration of the Questionnaire

As a first study, 100 paper-based questionnaires are distributed to the internet savvy students in order to know consumers' perception on electronic commerce adoption. The questionnaire are attached with a cover letter as shown in Appendix A, requesting cooperation from the respondents and promising them anonymity and confidentiality of their information. Since researcher did not have direct contact with most of the respondents, only 89 questionnaires are returned. Out of the questionnaires returned, 4 questionnaires were not usable because they were incomplete, such as more than 5 questions unanswered. Therefore, total of 85 questionnaires were reviewed and analyzed for the first study.

For the second study, the data utilized were collected using online survey instrument. The intended group of participants were the internet savvy general public. The survey link was posted on freesurveysonline.com and distributed to communities forums and blog of Malaysia's top e-commerce sites, namely, lelong.com.my, airasia.com and mphonline.com, for one month period. This online survey received 166 responses, of which 163 met the stated measure. Therefore, total of 163 questionnaires were reviewed and analyzed for the second study, and total of both studies (N: 85 + 163 = 248) were reviewed and analyzed for the overall study.

### 3.8 Analyzing Data

The analysis of data is carried out using the common Statistical Package for Social Sciences (SPSS for windows version 12.0). Descriptive analysis of the survey findings is presented in the first part of data analysis for the study I and II. In this part, responses are screened based on the demographic characteristics and the distributions of their responses to individual questions. Frequency distribution is used to explore the main characteristics of the respondents and their answers to individual questions.

Assessing the reliability of the scale used to measure the variables of interest is presented in the second part of data analysis for this study. Cronbach's alpha, which is derived from the average correlation of items inside a test if the items are consistent, is used for reliability coefficients.

Based on reliability test, factor analysis of the survey findings is computed. According to Coakes and Steed (1999), "more frequently, factor analysis is used as an exploratory technique when the researcher wishes to summarize the structure of a set of variables, p. 155." In addition, when the researchers' aim is to create a reliable test, factor analysis is an further means of determining whether items are tapping into the same construct.

Finally, tests of the research hypotheses using Pearson correlation coefficients and regression are involved as the final stage of data analysis for the study I and II. The data analysis plan is demonstrated in Figure 3.2.

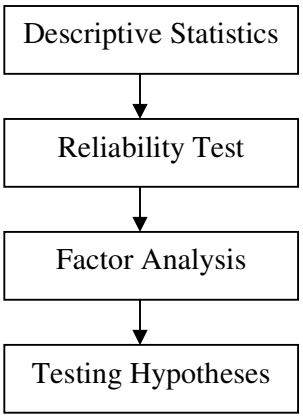



Figure 3.2. Stages of Data Analysis Adapted for this Study.

Using AMOS 18.0, Structural equation modeling (SEM) was conducted to validate the overall research model. A research model was established by the method of structural equation modeling (SEM). The SEM is based on several assumptions, such as consistency of measurements, and so on. With the collected data, the assumption was examined before conducting further analysis. Consistency of measurements was tested by examining the reliability. A common method of testing reliability is to calculate Cronbach's alpha. The generally agreed level of the Cronbach's alpha coefficient is 0.70 and above even though a coefficient level of 0.60 is acceptable in exploratory research.

After the assessment of the assumption, as the first step of the SEM, Confirmatory Factor Analysis (CFA) was executed. The next step was to conduct the SEM for the full model test, which is the combination of the structural model and measurement model. The sufficiency of the model was tested by utilizing the chi-square value, and several fit indices. Bagozzi and Yi, (1988) stated that the chi-square value is sensitive to a large sample (n>200). Chi-square/df should be used for the large sample size (n>200). As a rule of thumb, when chi-square/df is less than 3, the fit of a model could be judged by several model fit indices (e.g., GFI, CFI, NFI and RMSEA). By using AMOS 18.0, data analysis for SEM computed. Assumption tests for SEM and descriptive statistics were examined by SPSS 12.0 which is also used to test hypotheses by performing ANOVA.

### 3.9 Interview

In this study, besides survey data collection, we decided to conduct semi-structured interviews in order to know more about consumers' views on their perceptions related to e-commerce transactions. Our decision to include a qualitative method is supported by the fact that a qualitative method is useful in a condition where a rich amount of data is needed to create possibilities to understand the phenomenon as largely as possible and to produce new insights.

In addition to quantitative analysis as our main approach, we will also deploy the qualitative technique to support our quantitative findings. In the earlier section on data collection, we referred to the inclusion of questionnaire survey as main part of the data collected. Due to the nature of data, it seems more feasible to conduct a quantitative analysis that identifies the trend and pattern of the Internet and emerging technology usage and of the online shopping process than completely to deny the benefits of quantified information. Moreover, we pointed out that gathering consumers' perceptions could be achieved by the combination of quantitative and qualitative techniques. The results from our qualitative findings offer benefits in supporting our questionnaire analysis and also act as another source of information in our research process. Consequently, we consider that the conclusion generated from both methods gives us more confidence of our findings.

A semi-structured interview be capable of being much more flexible, letting the participant to transform the path of the conversation and suggest new issues that the interviewer had not defined. In a semi-structured interview, all participants are expected to remark about certain events. Participants might offer answers or give insight into events. Moreover, participants might support proof found from other sources. Hence, the interviewers have to stay away from going dependent on a particular respondent, and look for the similar data from other sources to confirm its validity.

We established a set of questions that related to our theoretical framework; however the nature of semi-structured interviews also has room for participants to elaborate their experiences and to express their opinions in a manner that is not

permitted by the pre-established interview questions. With this technique, we are more able to capture what we set out to explore with the established questions, as well as to give ourselves the freedom to take hold of other rich interpretations within our topic of investigation. We conducted 15 semi-structured interviews and each interview last on average between 45 minutes and 1 hour 30 minutes.

One issue related to interview is whether to use tape-recording. The recorded interviews give the researcher opportunity of having a record of conversations. Compared with note-taking interview, i.e. no tape-recording, it reduces the risk of missing out some key points raised by participants. However, one could argue that tape-recording interviews might inhibit participants to talk about sensitive issues since there is a psychological block of going on recording. Therefore, all the interviews were noted and fully transcribed.

To sum up, by using various types of information with both quantitative and qualitative techniques, we hope to express the credibility and dependability of this research.

## 3.10 Chapter Summary

In this chapter, the research framework has been entirely described, specifically, the theoretical model for testing the relationship between the variables and their hypothesized relationships. The main variables are also defined and their conceptual references stated where applicable. A model explaining the factors influencing consumers' trust in e-commerce transaction was derived and elaborated. In addition, the reasons for choosing both paper-based and online survey for data collection, target population, sampling, the development, design and construction of the questionnaire, reliability and validity testing of the survey instrument are explained in detail. The appropriateness of the SSPS and AMOS software and the statistical measures used in this study were described. A brief overview of semi-structured interviews of a qualitative research method was presented. The detail of the data analysis and findings will be given in the next chapter.

# CHAPTER 4

# DATA ANALYSIS AND RESULTS

## 4.1 Introduction

This chapter presents the results of the analysis of the consumers' trust in e-commerce adoption regarding their perceptions on security and privacy of their sensitive personal information, trustworthiness of web vendors and consumers' risk perception survey based on the research method described in the research methodology section of chapter three of this study. The findings of the survey together with the necessary statistical analysis will be explained in detail. The research findings will be examined based on two different parts, namely, non-online purchasers' perspectives and online purchasers' perspectives. The first section of each study will examine the responses to individual questions followed by the assessment of the reliability of the scale used to measure the variables of interest. Section three will examine the underlying structure of the variables of interest using factor analysis. Lastly, the relationship between the variables and tests the research hypotheses proposed in chapter three of this thesis will be examined in the concluding section of each study.

The purpose of this study was to research consumers' perceptions on security and privacy issues, trust and reliability of web vendors, and consumers' risk perceptions as they pertain to adopt e-commerce. Descriptive frequencies were provided for the respondents' demographic characteristics of gender, age, race, education and occupations. The analysis also provided descriptive frequencies for the following research constructs, namely, perceived security, perceived privacy, trustworthiness of web vendors, and perceived risk. The assessment of the reliability of the scale used to measure the variables of interest and the underlying structure of the variables of interest were examined for the research constructs. Pearson correlation coefficients

and regression analysis were computed to test the relationship between the variables and the research hypotheses proposed.

Responses to individual variables intended at finding factors related to the consumers' trust in e-commerce adoption as a research objective was explored in the next section.

## 4.2 Study I – Non-Online Purchasers' Perspectives

In first study of this survey, the target group of the respondents were the internet users who were non-online purchasers. 85 full-time final year undergraduate students from two local universities were participated in this study.

### 4.2.1 Sample Demographics

#### *4.2.1.1 Gender*

Based on respondents' responses, the respondents were much balanced in terms of gender as shown in Table 5.1, even though the number of male respondents was a bit higher than that of the female respondents. According to demographics, out of 85 respondents who responded to this survey, 43 were male representing 50.6% of the overall respondents whereas 42 were female representing 49.4% of the overall respondents.

#### *4.2.1.2 Age Groups*

The highest numbers of respondents were aged between 20 years and 30 years of age as exhibited in Table 4.1. Out of 85 respondents, the majority groups of the respondents (about 98.8%) were aged between 20 years old and 30 years old. The remaining (about 1.2%) were adults in their early 31's.

#### *4.2.1.3 Race*

The majority of the respondents from this survey were *Malay* race, representing 57.6% of the overall respondents followed by the *Chinese* race, representing about

18.8% of the total respondents. The remaining respondents consisted of Indian (about 15.3%) and other races (about 8.2%) as shown in Table 4.1.

Table 4.1
Summary on Respondents' Demographics

| Demographics | Frequency | Valid % |
|---|---|---|
| Gender | | |
| • Male | 43 | 50.6 |
| • Female | 42 | 49.4 |
| Age | | |
| • 20-30 | 84 | 98.8 |
| • 31-40 | 1 | 1.2 |
| Race | | |
| • Malay | 49 | 57.6 |
| • Chinese | 16 | 18.8 |
| • Indian | 13 | 15.3 |
| • Others | 7 | 8.2 |

### 4.2.2 Frequency of Internet Use and Purchases on the Internet

One of the objectives of this study was to get information related to respondents' frequency of Internet use and frequency of online purchases. Based on this objective, respondents were asked about their frequency of Internet use and frequency of purchases through the Internet. As shown in Table 4.2, the responses showed that even though most of the respondents frequently use the Internet, the respondents did not have experienced in online purchases. Out of the 85 respondents, almost all the respondents (about 96.5%) reported that they frequently use the Internet while the remaining 3.5% seldom use the Internet.

Table 4.2
Summary on Respondents' Frequency of Internet Use and Online Purchases

| Responses | Frequency of Internet use | | Frequency of online purchases | |
|---|---|---|---|---|
| | Frequency | Valid % | Frequency | Valid % |
| Always | 73 | 85.9 | 0 | 0 |
| Sometimes | 9 | 10.6 | 0 | 0 |
| Seldom | 3 | 3.5 | 0 | 0 |
| Never | 0 | 0 | 0 | 0 |
| Total | 85 | 100 | 0 | 0 |

### 4.2.3 Purchase Intention and Opinion on Credit Card Security

The respondents, who have not yet made online purchases, were asked about the possibility of their willingness to make online purchases in the near future. Out of 85 respondents who never purchase online before, about 49.4% were not willing to purchase in the near future, about 22.4% were willing to make online purchases but to a lesser amount and the remaining numbers of the respondents were willing to make more online purchases in the near future as shown in Table 4.3.

Table 4.3
Summary on Respondents' Frequency of the Willingness to Purchase Online in the Next Six Months

| Responses | Intention to purchase | |
|---|---|---|
| | Frequency | Valid % |
| I do not do this | 42 | 49.4 |
| Somewhat less | 19 | 22.4 |
| About the same | 17 | 20.0 |
| Somewhat more | 6 | 7.1 |
| Much more | 1 | 1.2 |
| Total | 85 | 100 |

Furthermore, the respondents who never purchased previously and also who were not willing to purchase online in the near future were asked about the reason for not buying online. As exhibited in Table 4.4, the major reason (about 36.5%) was cited to be the concern on security and privacy of their personal data, about 8.2% were due to lack of time, about 27.1% were because of lack of interaction, about 22.4% were because of cannot feel the product, about 2.4% were because of the high prices, and the remaining about 3.5% were due to other reasons.

Table 4.4
Summary on Respondents' Reasons for Not Buying Online

| Responses | Reasons for Not Buying Online | |
|---|---|---|
| | Frequency | Valid % |
| Security/Privacy | 31 | 36.5 |
| Lack of time | 7 | 8.2 |
| Lack of interaction | 23 | 27.1 |
| Can't feel product | 19 | 22.4 |
| High prices | 2 | 2.4 |
| Other | 3 | 3.5 |
| Total | 85 | 100 |

All respondents were also asked about the opinion on credit card security for online purchases. As shown in Table 4.5, the majority of the total respondents (about 54.1%) had the beliefs that the use of credit card for online purchases is unsafe, while about 11.8% believed somewhat safe. About 8.2% of the total respondents were indifferent for online credit card security and the remaining (24.7%) of the respondents were not sure about this.

Table 4.5
Summary on Respondents' Opinion on Credit Card Security

| Responses | Opinion on Credit Card security | |
|---|---|---|
| | Frequency | Valid % |
| Very Unsafe | 22 | 25.9 |
| Somewhat Unsafe | 24 | 28.2 |
| Indifferent | 7 | 8.2 |
| Somewhat Safe | 10 | 11.8 |
| Very Safe | 1 | 1.2 |
| Don't know | 21 | 24.7 |
| Total | 85 | 100 |

#### 4.2.4 Perceived Information Security

Regarding online information security concerns, only 10.6% of the respondents agreed that "they will feel totally safe providing sensitive information about themselves over the web" while majority (about 57.7%) of the respondents did not believe this, and about 31.8% of the respondents remained neutral on this question. On the online payment, about 22.4% of the respondents agreed that "the payment information they enter online is safe and accessible only by the intended persons" while majority (about 41.1%) of the respondents did not believe this. The remaining 36.5% of the respondents remained indifferent to the question. On the integrity of the online transactions, only 11.8% of the respondents believed that "the information they enter online is not altered in transit" while 33.0% of the respondents did not believe this. The remaining majority (about 55.3%) of the respondents remained neutral on this question. About 17.6% of the respondents agreed that "they will not hesitate to make purchase from the web because of security issues of sensitive information" and about 40.0% of the respondents did not agree this. The remaining 42.4% of the respondents remained indifferent to the question. Overall, about 31.8% of the respondents believed that "there is an adequate control in place to ensure security of personal data transmitted during online transaction processing" while about 30.6% of the respondents did not believe on this, and about 37.6% of the respondents remained neutral on this question.

Table 4.6
Responses on Perceived Information Security

| Response | Feel Safe Info | | Intended Recipient | | Not Altered in Transit | | Not Hesitate To Purchase | | Adequate Control | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Freq. | % | Freq. | % | Freq. | % | Freq. | % | Freq. | % |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| St. disagree | 19 | 22.4 | 7 | 8.2 | 5 | 5.9 | 10 | 11.8 | 4 | 4.7 |
| Disagree | 30 | 35.3 | 28 | 32.9 | 23 | 27.1 | 24 | 28.2 | 22 | 25.9 |
| Neutral | 27 | 31.8 | 31 | 36.5 | 47 | 55.3 | 36 | 42.4 | 32 | 37.6 |
| Agree | 5 | 5.9 | 18 | 21.2 | 10 | 11.8 | 11 | 12.9 | 19 | 22.4 |
| St. agree | 4 | 4.7 | 1 | 1.2 | 0 | 0 | 4 | 4.7 | 8 | 9.4 |
| Total | 85 | 100 | 85 | 100 | 85 | 100 | 85 | 100 | 85 | 100 |

There was no significant difference between the mean score of the items related to information security concerns, which ranged from 2.31 to 2.96. The standard deviations for the mean values ranged from 0.746 to 0.939. Among the five items, consumers' beliefs on "the information they enter online is not altered in transit" had lowest standard deviation that was 0.746 with mean value of 2.73 and "consumers will feel totally safe providing sensitive information about themselves over the web" had highest standard deviation, which was 0.939 with mean value of 2.31.

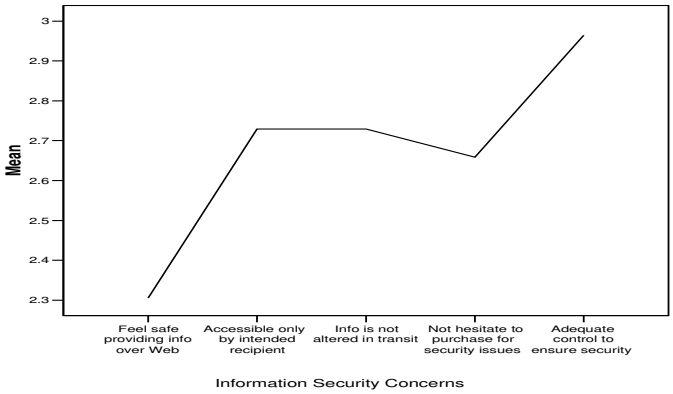



Figure 4.1. Mean value in Relation to Perceived Information Security.

### 4.2.5 Perceived Information Privacy

Regarding the information misused, about 36.5% of the respondents believed that "their personal information will not be misused when transacting with online companies" and about 23.5% of the respondents did not believe this. The remaining 40.0% of the respondents remained neutral on the question. Regarding the control over information, about 42.3% of the respondents believed that "they have control over how the information they provide will be used by online companies" while about 24.7% of the respondents did not believe this. The remaining 32.9% of the

respondents remained indifferent to the question. Moreover, about 31.8% of the respondents believed that "they can later verify the information they provide during a transaction with online companies" while about 24.7% of the respondents did not believe this. The remaining 43.5% of the respondents remained neutral on the question. In addition, only 25.9% of the respondents believed that "online companies will not reveal their sensitive information without their consent" while about 30.6% of the respondents did not believe this, and majority (about 43.5%) of the respondents remained neutral on this question.

Regarding the effective mechanism, about 35.3% of the respondents believed that "there is an effective mechanism to address any violation of the sensitive information they provide to online companies" while about 20.0% of the respondents did not believe this. The remaining majority (about 44.7%) of the respondents remained indifferent to the question. Overall, about 35.3% of the respondents believed that "there is an adequate control in place to protect the privacy of personal information within online companies" while about 18.8% of the respondents did not believe this, and majority (about 45.9%) of the respondents remained indifferent to this question.

Table 4.7
Responses on Perceived Information Privacy

| Response | Info Not Misused | | Control Info | | Verify Info | | No Reveal Info | | Effective Mech. | | Adequate control | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Frq. | % | Frq. | % | Frq. | % | Frq. | % | Frq. | % | Frq. | % |
| St. disagr | 4 | 4.7 | 4 | 4.7 | 4 | 4.7 | 7 | 8.2 | 5 | 5.9 | 4 | 4.7 |
| Disagree | 16 | 18.8 | 17 | 20.0 | 17 | 20.0 | 19 | 22.4 | 12 | 14.1 | 12 | 14.1 |
| Neutral | 34 | 40.0 | 28 | 32.9 | 37 | 43.5 | 37 | 43.5 | 38 | 44.7 | 39 | 45.9 |
| Agree | 23 | 27.1 | 24 | 28.2 | 22 | 25.9 | 16 | 18.8 | 27 | 31.8 | 24 | 28.2 |
| St. agree | 8 | 9.4 | 12 | 14.1 | 5 | 5.9 | 6 | 7.1 | 3 | 3.5 | 6 | 7.1 |
| Total | 85 | 100 | 85 | 100 | 85 | 100 | 85 | 100 | 85 | 100 | 85 | 100 |

There was no significant difference between the mean score of the items related to information privacy concerns, which ranged from 2.87 to 3.13. The standard deviations for the mean values ranged from 0.822 to 0.910. Among the six items, consumers' beliefs on "there is an adequate control in place to protect the privacy of personal information" had lowest standard deviation of 0.822 with mean value of 3.12 and consumers' beliefs on "there is an effective mechanism to address any violation of the sensitive information they provide" had highest standard deviation of 0.910 with mean value of 3.13.

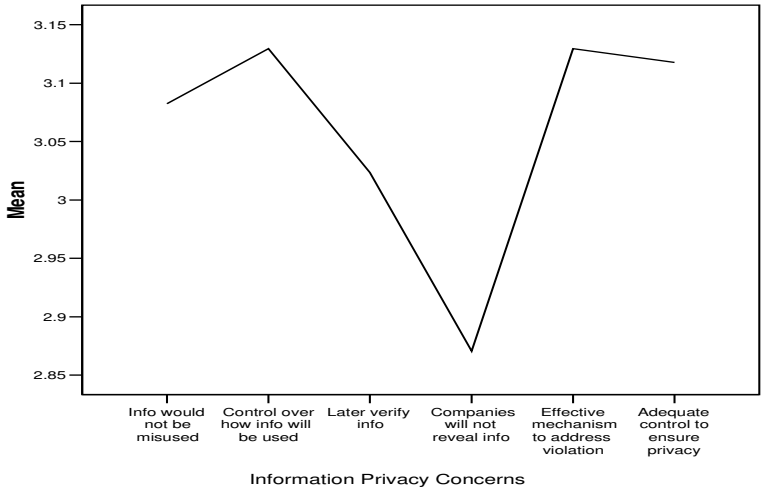



Figure 4.2. Mean value in Relation to Perceived Information Privacy.

### 4.2.6 Trustworthiness of Web Vendors

Regarding the trustworthiness of web vendors, about 36.5% of the respondents believed that "online companies will act with high business standards" while about 24.7% of the respondents did not believe this. The remaining 38.8% of the respondents remained indifferent to the question. On the skills and expertise, majority (about 48.2%) of the respondents believed that "online companies have the skills and expertise to perform transactions in an expected manner" and about 22.3% of the respondents did not believe this. The remaining 29.4% of the respondents remained neutral on the question. Regarding whether online companies are dependable, about 30.6% of the respondents believed that "online companies are dependable" while

about 24.7% of the respondents did not believe this. The remaining 44.7% of the respondents remained indifferent to the question. Moreover, about 29.4% of the respondents believed that "online companies do not have ill intensions about any of their consumers" while about 31.7% of the respondents did not believe this. The remaining 38.8% of the respondents remained indifferent to the question. Overall, only 22.4% of the respondents believed that "online companies are trustworthy" while about 25.9% of the respondents did not believe this, and majority (about 51.8%) of the respondents remained neutral on this question.

Table 4.8
Responses on Trustworthiness of Web Vendors

| Response | Business Standards | | Skill & Expertise | | Dependable | | No ill Intention | | Trustworthy | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Frq. | % | Frq. | % | Frq. | % | Frq. | % | Frq. | % |
| St. disagree | 5 | 5.9 | 4 | 4.7 | 4 | 4.7 | 7 | 8.2 | 8 | 9.4 |
| Disagree | 16 | 18.8 | 15 | 17.6 | 17 | 20.0 | 20 | 23.5 | 14 | 16.5 |
| Neutral | 33 | 38.8 | 25 | 29.4 | 38 | 44.7 | 33 | 38.8 | 44 | 51.8 |
| Agree | 25 | 29.4 | 37 | 43.5 | 21 | 24.7 | 22 | 25.9 | 17 | 20.0 |
| St. agree | 6 | 7.1 | 4 | 4.7 | 5 | 5.9 | 3 | 3.5 | 2 | 2.4 |
| Total | 85 | 100 | 85 | 100 | 85 | 100 | 85 | 100 | 85 | 100 |

There was no significant difference between the mean score of the items related to trustworthiness of web vendors, which ranged from 2.88 to 3.21. The standard deviations for the mean values ranged from 0.859 to 0.926. Among the five items, consumers' beliefs on "online companies do not have ill intensions about any of their consumers" had highest standard deviation that was 0.926 with mean value of 2.89 while consumers' beliefs on "online companies are dependable" had lowest standard deviation, which was 0.859 with mean value of 3.02.

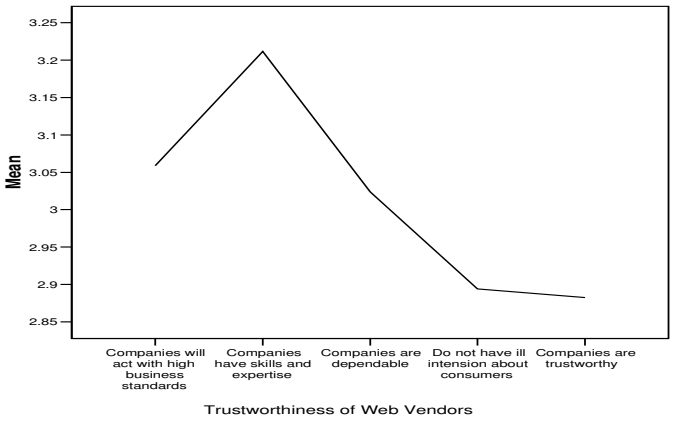



Figure 4.3. Mean value in Relation to Trustworthiness of Web Vendors.

### 4.2.7 Perceived Risk

Regarding risk perception, majority (about 48.3%) of the respondents believed that "providing credit card information over the web is unsafe" while only 18.8% of the respondents did not believe this. The remaining 32.9% of the respondents remained indifferent to the question. In addition, majority (about 54.1%) of the respondents believed that "it would be risky to give personal information to online companies" while about 17.7% of the respondents did not believe this. The remaining 28.2% of the respondents remained indifferent to the question. Furthermore, majority (about 51.7%) of the respondents agreed that "there would be too much uncertainty associated with providing personal information to online companies" and about 18.8% of the respondents did not agree on this. The remaining 29.4% of the respondents remained neutral on this question.

Table 4.9
Responses on Perceived Risk

| Response | Credit Card Unsafe | | Risky for Info | | Uncertainty for Info | |
|---|---|---|---|---|---|---|
| | Freq. | % | Freq. | % | Freq. | % |
| St. disagree | 5 | 5.9 | 2 | 2.4 | 1 | 1.2 |
| Disagree | 11 | 12.9 | 13 | 15.3 | 15 | 17.6 |
| Neutral | 28 | 32.9 | 24 | 28.2 | 25 | 29.4 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Agree | 23 | 27.1 | 38 | 44.7 | 33 | 38.8 |
| St. agree | 18 | 21.2 | 8 | 9.4 | 11 | 12.9 |
| Total | 85 | 100 | 85 | 100 | 85 | 100 |

There was no significant difference between the mean score of the items related to risk perception, which ranged from 3.46 to 3.51. The standard deviations for the mean values ranged from 0.894 to 1.031. Among the three items, "risky to give information over web" had lowest standard deviation of 0.894 with mean value of 3.46 and consumers' beliefs on "providing credit card information over the web is unsafe" had highest standard deviation of 1.031 with mean value of 3.51.

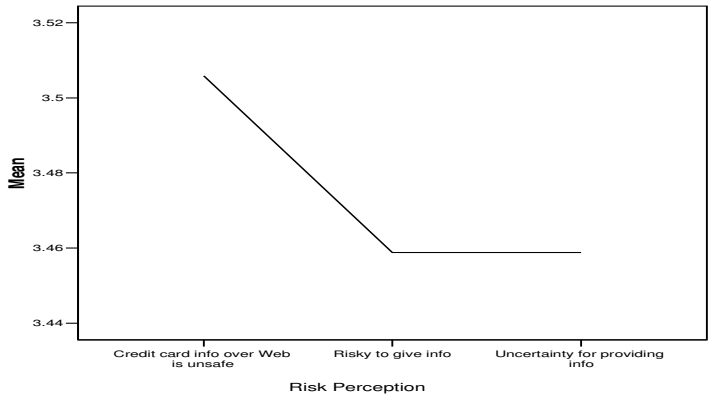



Figure 4.4. Mean value in Relation to Perceived Risk

### 4.2.8 Economic Incentives

Regarding economic incentives, about 24.7% of the respondents agreed that "providing credit card information over the web would not matter much if the prices are considerably lower" while about 38.8% of the respondents did not believe this. The remaining 36.5% of the respondents remained indifferent to the question. Furthermore, about 28.3% of the respondents agreed that "providing credit card information over the web would not matter much if the products/services are of a higher quality" and about 29.4% of the respondents did not agree on this. The remaining majority (about 42.4%) of the respondents remained neutral on this question. There was no significant difference between the mean score of the items

related to economic incentives, which were 2.91 and 3.14. The standard deviations for the mean values were 0.819 and 0.881.

### 4.2.9 Institutional Trust

Regarding institutional trust, about 55.3% of the respondents reported that "they will trust to open financial account with a bank" while about 17.6% did not agree on this and the remaining (about 27.1%) of respondents were not sure about this. Moreover, about 40.0% of the respondents reported that "they will trust to open financial account with a major credit card company" and only 8.2% of the respondents did not agree on this. The remaining majority (about 51.8%) of the respondents remained neutral on this question. There was no significant difference between the mean score of the items related to institutional trust, which were 3.45 and 3.54. The standard deviations for the mean values were 0.824 and 0.970.

Table 4.10
Responses on Economic Incentives and Institutional Trust

| Response | Low Price | | Higher Quality | | Trust with Bank | | Credit Card Company | |
|---|---|---|---|---|---|---|---|---|
| | Freq. | % | Freq. | % | Freq. | % | Freq. | % |
| St. disagree | 7 | 8.2 | 0 | 0 | 4 | 4.7 | 0 | 0 |
| Disagree | 26 | 30.6 | 21 | 24.7 | 11 | 12.9 | 7 | 8.2 |
| Neutral | 31 | 36.5 | 33 | 38.8 | 23 | 27.1 | 44 | 51.8 |
| Agree | 17 | 20.0 | 29 | 34.1 | 33 | 38.8 | 23 | 27.1 |
| St. agree | 4 | 4.7 | 2 | 2.4 | 14 | 16.5 | 11 | 12.9 |
| Total | 85 | 100 | 85 | 100 | 85 | 100 | 85 | 100 |

### 4.2.10 Consumers' Trust

On the use of more complex and advanced method, the majority (about 64.7%) of the respondents agreed 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" while only 9.5% did not agree on this and 25.9% of the respondents remained neutral on this question. On providing all necessary guarantees to increase consumers' confidence to adopt e-commerce, the majority (about 58.8%) of the

respondents agreed that "their confidence to adopt e-commerce will increase when online vendors provide all necessary guarantees to ensure security and privacy of their personal information" while only 8.2% did not agree on this and the remaining (about 32.9%) of respondents were not sure about this. There was no significant difference between the mean score of the items related to consumers' trust, which were 3.75 and 3.86. The standard deviations for the mean values were 0.925 and 0.966.

Table 4.11
Responses on Consumers' Trust

| Response | Advanced Method | | Necessary Guaranties | |
|---|---|---|---|---|
| | Freq. | % | Freq. | % |
| St. disagree | 2 | 2.4 | 0 | 0 |
| Disagree | 6 | 7.1 | 7 | 8.2 |
| Neutral | 22 | 25.9 | 28 | 32.9 |
| Agree | 29 | 34.1 | 29 | 34.1 |
| St. agree | 26 | 30.6 | 21 | 24.7 |
| Total | 85 | 100 | 85 | 100 |

### 4.2.11 Reliability Analysis

Reliability analysis was performed to assess the reliability of the scale used to measure the variables of interest. Reliability can be defined as the degree to which an instrument measures the same way each time it's used under the same conditions with the same subjects (Sproull, 1995). The reliability test in research assesses the degree of accuracy, consistency and predictability of measuring instruments in terms of their stability over time. There are several forms of reliability test. However, the internal consistency test was adopted for this study because it is the most commonly used measure of reliability. The internal consistency test assesses the degree to which items on a scale represent the concepts or measure the same construct.

Since no one item is a perfect measure of a construct, the assessment of internal consistency relies on a series of tests to determine coefficient of alpha for the items on the scale. The alpha measures the coefficient of correlation between items measuring the same construct. The generally agreed level of the Cronbach's alpha coefficient is 0.70 and above even though a coefficient level of 0.60 is acceptable in exploratory research.

Firstly, the reliability assessment of the entire scale was computed followed by the assessments of individual items supposed to measure the hypothesized research constructs based on factor analysis. The overall reliability assessment of the entire scale was observed to be with a Cronbach's alpha of 0.820, which is above the recommended level of alpha coefficient. A second test was conducted to assess the degree to which the items on the scale measure the hypothesized research constructs. A total of twenty five items measuring six constructs and one dependent variable (five items measuring Information Security Concerns, six items measuring Information Privacy Concerns, five items measuring Trust Beliefs of Web Vendors, three items measuring Risk Perception, two items measuring Economic Incentive, two items measuring Institutional Trust, and two items measuring Consumers' Trust in e-commerce transactions) were assessed for reliability (See Table 4.12).

Table 4.12
Reliability Analysis Results

| Construct | Means and SD | Alpha |
|---|---|---|
| Information Security Concerns | 13.39 (3.03) | 0.725 |
| Information Privacy Concerns | 18.35 (3.12) | 0.636 |
| Trust Beliefs of Web Vendors | 15.07 (2.91) | 0.660 |
| Risk Perception | 10.42 (2.20) | 0.642 |
| Economic Incentives | 6.05 (1.37) | 0.660 |
| Institutional Trust | 6.99 (1.63) | 0.779 |
| Consumers' Trust | 7.61 (1.66) | 0.707 |

### 4.2.12 Factor Analysis

After conducting reliability analysis to assess the reliability of the scale used to measure the variables of interest, factor analysis was performed to identify the underlying factors affecting consumers' confidence to adopt e-commerce. Factor analysis can be used to determine what items should be included on or excluded in further analysis. To make effective use of factor analysis in a study, the criteria, namely, a priori conceptual beliefs about the number of factors to include in factor analysis, the scree test, and the interpretability of the factor solution should be considered (Green and Salkind 2003).

Factor analysis is concerned with whether the covariances or correlarions between a set of observed variables can be explained in terms of a smaller number of unobservable constructs known as common factors (Landau and Everitt, 2004). Factor analysis is one of the most commonly used techniques for data reduction and structure detection in social science research, and moreover, it may also be used for deciding which items on the scale are to be included and excluded from the measure.

According to Hair et al. (2000), one of the conditions necessary for data to be analyzed using factor analysis is the variables should not be categorized as dependent and independent. As shown in the appendix E, both factor extraction and factor rotation were performed while conducting factor analysis for this study. Absolute magnitude of Eigenvalue was used to determine the number of factors to be extracted in the factor extraction stage. Factor extraction was followed by factor rotation using the most widely used method of factor rotation known as the Varimax rotation in order to make extracted factors easily interpretable.

In this study, factor analysis (factor extraction as well as varimax factor rotation) was conducted to identify the underlying factors affecting consumers' trust in e-commerce transactions. Considering all the 25 items on security and privacy of consumer's personal information, trust and reliability of web vendors, consumer's perceived risk, economics incentives, and institutional trust, were analyzed using principal component analysis. "Total Variance Explained" showed the extent to which total variance of the observed variables was explained by each of the principal components. Eigenvalues are helpful in deciding how many factors should be used in the analysis of study. Many criteria have been proposed in the literature for deciding how mnay factors to extract based on the magnitudes of eigenvalues. One of the criteria to determine the factors is to retain all factors that have eigenvalue greater than 1(Green and Salkind 2003). Initial factor extraction revealed seven components with an absolute magnitude of eigenvalue greater than 1.0.

As shown in Table 4.13, the first principal component, which related to the trust and reliability of web vendors, was the largest part of the total variance, had an eigenvalue of 5.504 amounted to 22.02% of the total variance. The second principal component, which related to the consumers' perceived security had a variance of

about 2.953 and accounted for a further 11.81% of the total variance. The third principal component was related to the consumers' perceived privacy, had an eigenvalue of 1.827 amounted to 7.32% of the total variance. The forth principal component, which related to the consumers' perceived risk had an eigenvalue of about 1.661 and accounted for 6.65% of the total variance. The fifth principal component, which related to the institutional trust had a variance of about 1.447 and accounted for a further 5.79% of the total variance. The six principal component was related to the consumers' trust in e-commerce transactions, had an eigenvalue of 1.324 amounted to 5.3% of the total variance. The seventh principal component, which related to the economic incentives, had an eigenvalue of about 1.181 and accounted for 4.73% of the total variance. In general, all the seven principal components together accounted for 63.596% of the total variance in the original 25 items.

Table 4.13
Total Variance Explained

| | Initial Eigenvalues | | |
|---|---|---|---|
| Component | Total | % of Variance | Cumulative % |
| 1 | 5.504 | 22.015 | 22.015 |
| 2 | 2.953 | 11.811 | 33.826 |
| 3 | 1.829 | 7.316 | 41.142 |
| 4 | 1.661 | 6.646 | 47.788 |
| 5 | 1.447 | 5.788 | 53.576 |
| 6 | 1.324 | 5.295 | 58.871 |
| 7 | 1.181 | 4.725 | 63.596 |

*Extraction Method: Principal Component Analysis.*

Most items loaded onto the extracted factors except from the some items that were conceptualized to measure the information security concerns, information privacy concerns and trust beliefs of web vendors. The item "adequate control to ensure security" fairly loaded onto the factor of trustworthiness of web vendors, while the item "companies do not have ill intention about consumers" slightly loaded onto the information security concerns factor. However, the items "later verify info" and "effective mechanism to address violation" of the information privacy concerns factor fairly loaded onto factor one (trustworthiness of web vendors). Also, the item "companies are dependable" of the trustworthiness of web vendors factor loaded onto

factor three. The tree items, namely, feel safe providing information over web, information would not be misused, and companies are trustworthy, had factor loading lower than 0.50. The results of factor analysis were shown in Table 4.14.

Table 4.14
Results of Factor Extraction and Factor Loading

| Items | F1 | F2 | F3 | F4 | F5 | F6 | F7 |
|---|---|---|---|---|---|---|---|
| Skills and expertise | 0.749 | | | | | | |
| Effective mechanism | 0.745 | | | | | | |
| Later verify Info | 0.694 | | | | | | |
| Business standards | 0.536 | | | | | | |
| Ensure security | 0.538 | | | | | | |
| Not hesitate to purchase | | 0.735 | | | | | |
| Info not altered | | 0.687 | | | | | |
| No ill intension | | 0.660 | | | | | |
| Intended recipient | | 0.534 | | | | | |
| Dependable | | | 0.669 | | | | |
| Not reveal Info | | | 0.629 | | | | |
| Ensure Privacy | | | 0.569 | | | | |
| Control over Info | | | 0.527 | | | | |
| Risky to give Info | | | | 0.780 | | | |
| Credit card unsafe | | | | 0.652 | | | |
| Uncertainty | | | | 0.619 | | | |
| Trust with company | | | | | 0.861 | | |
| Trust with bank | | | | | 0.792 | | |
| Necessary guaranties | | | | | | 0.690 | |
| Advance Method | | | | | | 0.548 | |
| Higher quality | | | | | | | 0.873 |
| Low price | | | | | | | 0.514 |

**4.2.13 Hypotheses Testing**

Firstly, pearson correlation coefficients was computed in order to test the relationships between each factor and consumers' trust in e-commerce transactions. The results showed that there is a very low correlation (r=0.067) between perceived security and consumers' trust in e-commerce adoption. This can be said that since consumers get familiar with the World Wide Web and with the emerging information technologies to safe and secure themselves in dealing with e-commerce transactions, their concerns on security issues are turning less significant matter from time to time. In addition, a very low positive correlation (r=0.002 with p>0.05) existed between

perceived privacy and consumers' trust in e-commerce adoption. It can be said that consumers might also get ready to follow defensive methods on themselves to care for their privacy in dealing with e-commerce transactions, such as giving untrue personal information to web vendors.

The construct of perceived privacy fairly manifested itself primarily through perceived security (r=0.424, p=0.000) on consumers' trust in e-commerce adoption. This may be because the privacy concern of online consumers will be less sensitive matter if they believe that they are transacting with secure mediums. A slight positive correlation (r=0.218, p<0.05) existed between trustworthiness of web vendors and consumers' trust in e-commerce transactions, which implies that trustworthiness of web vendors has slight impact on consumers' trust in e-commerce adoption. This can be said that consumers would prefer to transact with well-known vendors over the Internet. Moreover, the construct of perceived privacy fairly manifested itself primarily through trustworthiness of web vendors (r=0.449, p=0.000) on consumers' trust in e-commerce transactions. This may be because the privacy concern of non-online purchasers will be less sensitive matter if they transact with well-known vendors over the Internet.

There is a fair positive correlation (r=0.388, p=0.000) existed between perceived risk and consumers' trust in e-commerce adoption. Consumers would consider the trust beliefs they may have towards adoption of e-commerce and their risk perception. It was found that economic incentives and institutional trust have no impact on consumers' perceived risk. The results showed that the increase in economic incentives does not reduce a consumer's perceived risk in online transaction. The relationship is observed to be with $p > 0.05$. In addition, the increase in institutional trust does not reduce a consumer's perceived risk in online transaction. The relationship is observed to be $r = 0.148$ with $p = 0.176$, as shown in Table 4.15.

Table 4.15
Results of E-Commerce Adoption Factors Correlation

| | Security | Privacy | Vendor | Risk | Economic | Institute | Con_trust |
|---|---|---|---|---|---|---|---|
| Security | 1.000 | | | | | | |
| Privacy | 0.424 | 1.000 | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Vendor | 0.513 | 0.449 | 1.000 | | | | |
| Risk | -0.074 | -0.071 | 0.055 | 1.000 | | | |
| Economic | 0.144 | 0.134 | 0.269 | -0.077 | 1.000 | | |
| Institute | 0.239 | 0.121 | 0.357 | 0.148 | 0.245 | 1.000 | |
| Con_trust | 0.067 | 0.002 | 0.218 | 0.388 | 0.045 | 0.381 | 1.000 |

Secondly, a multiple regression analysis was conducted to evaluate the relationship between the predictors of consumers' perceived security, perceived privacy, trustworthiness of web vendors, and consumers' perceived risk with consumers' trust in e-commerce transactions. Table 4.16(i) through Table 4.16(iii) presented the results of multiple regression analysis computed for one dependent variable and the four predictors.

The linear combination of the consumers' perceived security, perceived privacy, trustworthiness of web vendors, and consumers' perceived risk was significantly related to the consumers' trust in e-commerce transactions, $F(4, 80) = 5.552$, $p<0.001$, as shown in Table 4.16(ii). The results showed that consumers' perceptions on security and privacy issues, trustworthiness of web vendors and issues related to consumers' risk perceptions will influence consumers' trust in e-commerce transactions or how soon they will adopt e-commerce in near future. The sample multiple correlation coefficients is 0.47, indicating that approximately 22% of the variance for the consumers' trust in e-commerce transactions in the sample can be accounted for by the linear combination of perceived security, perceived privacy, trustworthiness of web vendors, and perceived risk measures.

The regression analysis of this study showed that only two out of four predictors (trustworthiness of web vendors and consumers' perceived risk) were found to be significant ($p<0.05$ and $p<0.01$) to the consumers' trust in e-commerce adoption. In overall, the regression model showed about 18.0% (Adjusted R Square = 0.178) of the consumers' trust in e-commerce adoption will be influenced by the consumers' perceived security, perceived privacy, trustworthiness of web vendors, and consumers' perceived risk.

Table 4.16(i)
Regression Model Summary

| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate |
|---|---|---|---|---|
| 1 | 0.466 | 0.217 | 0.178 | 0.75362 |

Predictors: (Constant), Perceived Security, Perceived Privacy, Beliefs of Web Vendors, Perceived Risk

Dependent Variable: Consumers' Trust in E-commerce Transactions

Table 4.16(ii)
ANOVA

| Model | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| 1 | Regression | 12.612 | 4 | 3.153 | 5.552 | 0.001 |
| | Residual | 45.435 | 80 | 0.568 | | |
| | Total | 58.047 | 84 | | | |

Predictors: (Constant), Perceived Security, Perceived Privacy, Beliefs of Web Vendors, Perceived Risk

Dependent Variable: Consumers' Trust in E-commerce Transactions

Table 4.16(iii)
Predictors Coefficients

| | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
|---|---|---|---|---|---|
| | B | Std. Error | Beta | | |
| (Constant) | 1.995 | 0.648 | | 3.077 | 0.003 |
| Perceived security | -0.241 | 0.157 | -0.184 | -1.540 | 0.127 |
| Perceived privacy | -0.046 | 0.161 | -0.033 | -0.284 | 0.777 |
| Beliefs of web vendors | 0.394 | 0.156 | 0.307 | 2.527 | 0.013 |
| Risk perception | 0.404 | 0.114 | 0.355 | -3.550 | 0.001 |

Dependent Variable: Consumers' Trust in E-commerce Transactions

A multiple regression analysis was also conducted to evaluate the relationship between the predictors of economic incentives and institutional trust with consumers' perceived risk. Table 4.17(i) through Table 4.17(iii) presented the results of multiple regression analysis computed for risk as dependent variable and the two predictors which are economic incentives and institutional trust. The linear combination of the economic incentives and institutional trust was not significantly related to the consumers' perceived risk $F(2, 82) = 1.515$, $p>0.05$ as shown in Table 4.17(ii). The results showed that the increase on economic incentives and institutional trust will not reduce consumers' perceived risk. The sample multiple correlation coefficients is 0.19, indicating that only 3.6% of the variance for the consumers' perceived risk in the

sample can be accounted for by the linear combination of economic incentives and institutional trust measures.

The regression analysis of this study showed that the two predictors were found to be insignificant to the consumers' perceived risk. In overall, the regression model showed only 1.2% (Adjusted R Square = 0.012) of the consumers' perceived risk will be influenced by economic incentives and institutional trust.

Table 4.17(i)
Regression Model Summary

| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate |
|---|---|---|---|---|
| 1 | 0.189 | 0.036 | 0.012 | 0.72763 |

Predictors: (Constant), Economic incentives, Institutional trust
Dependent Variable: Consumers' perceived risk

Table 4.17(ii)
ANOVA

| Model | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| 1 | Regression | 1.604 | 2 | 0.802 | 1.515 | 0.226 |
| | Residual | 43.414 | 82 | 0.529 | | |
| | Total | 45.018 | 84 | | | |

Predictors: (Constant), Economic incentives, Institutional trust
Dependent Variable: Consumers' perceived risk

Table 4.17(iii)
Predictors Coefficients

| | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
|---|---|---|---|---|---|
| | B | Std. Error | Beta | | |
| (Constant) | 3.306 | 0.445 | | 7.432 | 0.000 |
| Economic incentives | -0.129 | 0.119 | -0.121 | -1.078 | 0.284 |
| Institutional trust | 0.160 | 0.101 | 0.178 | 1.589 | 0.116 |

Dependent Variable: Consumers' perceived risk

**H1:** A consumer's perceived security of online transaction positively influences his/her trust in online transaction.

The result of the study showed that perceived security does not affect the consumers' trust in e-commerce adoption. The correlation coefficient between consumers' perceived security towards online transaction and their confidence to adopt e-commerce was found to be with ($r = -0.067$, $p>0.05$). Therefore, the research hypothesis was not supported.

**H2:** A consumer's perceived privacy of online transaction positively influences his/her trust in online transaction.

The result of the study showed that perceived privacy does not influence the consumers' trust in e-commerce adoption. The relationship was observed to be with ($r = 0.002$, $p > 0.05$). Therefore, the research hypothesis was not supported.

**H3:** A consumer's perceived privacy of online transaction positively influences perceived security of online transaction.

The result of the study showed that consumer's perceived privacy of online transaction on trust was mediated by perceived security ($r = 0.424$). The relationship was observed to be statistically significant with significance level less than 0.01 ($p = 0.000$). Therefore, the research hypothesis was supported.

**H4:** The trustworthiness of web vendor positively influences a consumer's trust in online transaction.

The results of the study showed that trustworthiness of web vendor influence the consumers' trust in e-commerce adoption. The relationship was observed to be statistically significant ($r = 0.218$, $p < 0.05$). Given the significant positive relationship between trustworthiness of web vendors and the consumers' confidence to adopt e-commerce, there was a reason to believe that the research hypothesis was significantly supported.

**H5:** A consumer's perceived privacy of online transaction positively influences the trustworthiness of web vendor of online transaction.

The result of the study showed that consumer's perceived privacy of online transaction on trust was mediated by trustworthiness of web vendor ($r = 0.449$). The

relationship was observed to be statistically significant with significance level less than 0.01 ($p = 0.000$). Therefore, the research hypothesis was supported.

**H6:** A consumer's perceived risk in online transaction positively influences his/her trust in online transaction.

The results of the study showed that a consumer's perceived risk in online transaction positively influences his/her trust in online transaction ($r = 0.388$). The relationship was observed to be statistically significant with significance level less than 0.01.

**H7:** The increase in economic incentives reduces consumers' perceived risk in online transaction.

We found that the increase in economic incentives did not reduce a consumers' perceived risk in online transaction. The relationship was observed to be with $p > 0.05$. Therefore, the research hypothesis was not supported.

**H8:** The increase in institutional trust reduces consumers' perceived risk in online transaction.

We also found that the increase in institutional trust did not reduce a consumers' perceived risk in online transaction. The relationship was observed to be with ($r = 0.148$, $p > 0.05$). Therefore, the research hypothesis was not supported.

### 4.3 Study II – Online Purchasers' Perspectives

In this online survey, the data utilized were collected using online survey instrument. The target group of respondents were the internet savvy general public. The survey link was posted on freesurveysonline.com and distributed to communities' forums and blogs of Malaysia's top e-commerce sites, namely, lelong.com.my, airasia.com and mphonline.com, for one month period.

#### 4.3.1 Sample Demographics

One hundred and sixty three respondents (62.0% males and 38.0% females) were participated for the purpose of analysis for this study. The majority of the respondents

(about 81.0%) were age between 20 to 30, followed by age between 31 to 40 (about 17.8%), while remaining about 1.2% are age between 41 to 50. The results showed that the sample was skewed towards age between 20 to 30, with the mean of 1.2 and standard deviation of 0.433. In term of races, about 54.0% were Malay, followed by Chinese race (about 23.3%), while about 12.9% were Indian and about 9.8% were other races.

The majority of the respondents who participated in the survey were highly educated with most of the sample being degree holders. Out of the overall respondents, about 28.2% of the respondents had graduated at the diploma level, about 54.0% of the respondents were holding university degrees, and 17.2% of the respondents had master's degrees. The remaining numbers of the respondents (about 0.6%) were holding high school or certificates. The respondents were having worked for different departments in a variety of positions such as administration, management, educator, sales personnel, and professional. The majority (about 46.0%) of the respondents were working in management level, followed by administrative assistants (about 21.5%). About 14.1% were working as sales personnel, educators (about 11.7%), and the remaining respondents were professional (about 6.7%) as shown in Table 4.18.

Table 4.18
Respondents' Demographic Information

| Variables | Frequency | Percent |
|---|---|---|
| Gender | | |
| • Male | 101 | 62.0 |
| • Female | 62 | 38.0 |
| Age group | | |
| • 20 -30 years | 132 | 81.0 |
| • 31-40 years | 29 | 17.8 |
| • 41-50 years | 2 | 1.2 |
| • 51 years and above | 0 | 0 |
| Race | | |
| • Malay | 88 | 54.0 |
| • Chinese | 38 | 23.3 |
| | 21 | 12.9 |

| | | |
|---|---|---|
| • Indian<br>• Others | 16 | 9.8 |
| Highest level of education | | |
| • High school | 1 | 0.6 |
| • Diploma | 46 | 28.2 |
| • Bachelors | 88 | 54.0 |
| • Masters | 28 | 17.2 |
| • Ph.D | 0 | 0 |
| • Others | 0 | 0 |
| Occupation | | |
| • Administrative Support | 35 | 21.5 |
| • Management | 75 | 46.0 |
| • Educator | 19 | 11.7 |
| • Sales Personnel | 23 | 14.1 |
| • Professional | 11 | 6.7 |
| • Others | 0 | 0 |

### 4.3.2 Responses on Various E-Commerce Issues

Out of the 163 online respondents, almost all the respondents (about 96.9%) reported that they frequently use the internet while the remaining 3.1% sometimes use the internet. The observation of the responses showed that respondents (about 50.3%) made online purchases sometimes, followed by made online purchases seldom (about 49.1%), while only 0.6% made online purchases always. Out of the respondents who had purchased online previously, majority (about 52.1%) had made purchases between 1 year and 3 years, about 33.7% had made purchases between 4 years and 6 years, and about 14.1% had made purchases for less than 1 year.

The respondents, who had made purchases on the Internet, were also asked about the possibility of continued purchasing in the near future compared to previous purchases. Only 1.8% of the respondents were willing to reduce their future purchases compared to previous purchases, while majority (about 67.5%) were willing to maintain the same status by neither increasing nor decreasing their online purchases. About 30.7% were willing to make a bit more online purchases in the near future.

All the respondents were also asked about their opinion on credit card security for online purchases. The majority of the respondents (about 60.1%) believed that “the use of credit card for online purchases is somewhat safe” while about 22.1% believed

"somewhat unsafe". About 15.3% of the respondents were indifferent on online credit card security and the remaining (about 2.5%) respondents believed "very safe" as shown in Table 4.19.

Table 4.19
Responses on Various E-Commerce Issues

| Issues | Frequency | Percent |
|---|---|---|
| How long have you been purchasing online? | | |
| • Less than 1 year | 23 | 14.1 |
| • Between 1 and 3 years | 85 | 52.1 |
| • Between 4 and 6 years | 55 | 33.7 |
| • More than 6 years | 0 | 0 |
| Willingness to continue online purchases within the next 6 months (those who have experienced in purchasing online) | | |
| • I will not do this | 0 | 0 |
| • Somewhat less | 3 | 1.8 |
| • About the same | 110 | 67.5 |
| • Somewhat more | 50 | 30.7 |
| • Much more | 0 | 0 |
| Credit card security | | |
| • Very unsafe | 0 | 0 |
| • Somewhat unsafe | 36 | 22.1 |
| • Indifferent | 25 | 15.3 |
| • Somewhat safe | 98 | 60.1 |
| • Very safe | 4 | 2.5 |

### 4.3.3 Perceived Information Security

Regarding online information security concerns, about 57.7% of the respondents agreed that "they will feel totally safe providing sensitive information about themselves over the web" while about 42.3% of the respondents remained neutral on this question. Regarding the online payment, majority (about 78.5%) of the respondents agreed that "the payment information they enter online is safe and accessible only by the intended persons" while the remaining 21.5% of the respondents remained indifferent to the question. On the integrity of the online transactions, majority (about 63.8%) of the respondents believed that "the information they enter online is not altered in transit" while the remaining about 36.2% of the respondents remained neutral on this question. About 74.8% of the respondents agreed that "they will not hesitate to make purchase from the web because of security

issues of sensitive information" and about 25.2% of the respondents remained indifferent to the question. Overall, about 79.1% of the respondents believed that "there is an adequate control in place to ensure security of personal data transmitted during online transaction processing" while about 20.9% of the respondents remained neutral on this question.

Table 4.20
Responses on Perceived Information Security

| Response | Feel Safe Info | | Intended Recipient | | Not Altered in Transit | | Not Hesitate To Purchase | | Adequate Control | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Freq. | % | Freq. | % | Freq. | % | Freq. | % | Freq. | % |
| St. disagree | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Disagree | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Neutral | 69 | 42.3 | 35 | 21.5 | 59 | 36.2 | 41 | 25.2 | 34 | 20.9 |
| Agree | 94 | 57.7 | 128 | 78.5 | 104 | 63.8 | 122 | 74.8 | 129 | 79.1 |
| St. agree | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total | 163 | 100 | 163 | 100 | 163 | 100 | 163 | 100 | 163 | 100 |

As shown in Table 4.21, there was no significant difference between the mean score of the items related to information security concerns, which ranged from 3.58 to 3.79. The standard deviations for the mean values ranged from 0.408 to 0.496. Among the five items, consumers' beliefs on adequate control to ensure security had lowest standard deviation that was 0.408 with mean value of 3.79 and consumers' beliefs on safety of providing information over web had highest standard deviation that was 0.496 with mean value of 3.58.

Table 4.21
Mean Value and Standard Deviation for the Items of Perceived Information Security

| Items | Mean | Std. Deviation |
|---|---|---|
| Feel safe providing info over web | 3.58 | 0.496 |
| Accessible only by intended recipient | 3.79 | 0.412 |
| Info is not altered in transit | 3.64 | 0.482 |
| Not hesitate to purchase for security issues | 3.75 | 0.435 |

| | | |
|---|---|---|
| Adequate control to ensure security | 3.79 | 0.408 |

### 4.3.4 Perceived Information Privacy

Regarding the information misused, about 46.6% of the respondents believed that "their personal information will not be misused when transacting with online companies" and about 53.4% of the respondents remained neutral on the question. Regarding the control over information, about 36.8% of the respondents believed that "they have control over how the information they provide will be used by online companies" while majority (about 63.2%) of the respondents remained indifferent to the question. Moreover, majority (about 80.4%) of the respondents believed that "they can later verify the information they provide during a transaction with online companies" while about 19.6% of the respondents remained neutral on the question. In addition, about 45.4% of the respondents believed that "online companies will not reveal their sensitive information without their consent" while about 54.6% of the respondents remained neutral on this question. Regarding the effective mechanism, about 59.5% of the respondents believed that "there is an effective mechanism to address any violation of the sensitive information they provide to online companies" while about 40.5% of the respondents remained indifferent to the question. Overall, about 71.2% of the respondents believed that "there is an adequate control in place to protect the privacy of personal information within online companies" while about 28.8% of the respondents remained indifferent to this question.

Table 4.22
Responses on Perceived Information Privacy

| Response | Info Not Misused | | Control Info | | Verify Info | | No Reveal Info | | Effective Mech. | | Adequate control | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Frq | % | Frq | % | Frq | % | Frq | % | Frq | % | Frq | % |
| St. disagr | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Disagree | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Neutral | 87 | 53 | 103 | 63 | 32 | 20 | 89 | 55 | 66 | 41 | 47 | 29 |
| Agree | 76 | 47 | 60 | 37 | 131 | 80 | 74 | 45 | 97 | 60 | 116 | 71 |
| St. agree | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Total | 163 | 100 | 163 | 100 | 163 | 100 | 163 | 100 | 163 | 100 | 163 | 100 |

There was no significant difference between the mean score of the items related to information privacy concerns, which ranged from 3.37 to 3.80. The standard deviations for the mean values ranged from 0.398 to 0.500. Among the six items, consumers' beliefs on "can later very information" had lowest standard deviation of 0.398 with mean of 3.80 and consumers' beliefs on "information will not be misused" had highest standard deviation of 0.500 with mean value of 3.47 as shown in Table 4.23.

Table 4.23
Mean Value and Standard Deviation for the Items of Perceived Information Privacy

| Items | Mean | Std. Deviation |
|---|---|---|
| Info will not be misused | 3.47 | 0.500 |
| Control over how info will be used | 3.37 | 0.484 |
| Later verify info | 3.80 | 0.398 |
| Companies will not reveal info | 3.45 | 0.499 |
| Effective mechanism to address violation | 3.60 | 0.492 |
| Adequate control to ensure privacy | 3.71 | 0.454 |

### 4.3.5 Trustworthiness of Web Vendors

Regarding trustworthiness of web vendors, about 44.2% of the respondents believed that "online companies will act with high business standards" while about 55.8% of the respondents remained indifferent to the question. On the skills and expertise, majority (about 74.8%) of the respondents believed that "online companies have the skills and expertise to perform transactions in an expected manner" and about 25.2% of the respondents remained neutral on the question. Regarding whether online companies are dependable, about 27.0% of the respondents believed that "online companies are dependable" while majority (about 73.0%) of the respondents remained indifferent to the question. Moreover, about 21.5% of the respondents believed that "online companies do not have ill intensions about any of their

consumers" while majority (about 78.5%) of the respondents remained indifferent to the question. Overall, only 21.5% of the respondents believed that "online companies are trustworthy" while majority (about 78.5%) of the respondents remained neutral on this question.

Table 4.24
Responses on Trustworthiness of Web Vendors

| Response | Business Standards | | Skill & Expertise | | Dependable | | No ill Intention | | Trustworthy | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Frq. | % | Frq. | % | Frq. | % | Frq. | % | Frq. | % |
| St. disagree | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Disagree | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Neutral | 91 | 55.8 | 41 | 25.2 | 119 | 73.0 | 128 | 78.5 | 128 | 78.5 |
| Agree | 72 | 44.2 | 122 | 74.8 | 44 | 27.0 | 35 | 21.5 | 35 | 21.5 |
| St. agree | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total | 163 | 100 | 163 | 100 | 163 | 100 | 163 | 100 | 163 | 100 |

There was no significant difference between the mean score of the items related to trustworthiness of web vendors, which ranged from 3.21 to 3.75. The standard deviations for the mean values ranged from 0.412 to 0.498. Among the five items, consumers' beliefs on "online companies will act with high business standards" had highest standard deviation of 0.498 with mean value of 3.44 while consumers' beliefs on "online companies do not have ill intensions" and "online companies are trustworthy" had lowest standard deviation of 0.412 with mean value of 3.21 (See Table 4.25).

Table 4.25
Mean Value and Standard Deviation for the Items of Trustworthiness of Web Vendors

| Items | Mean | Std. Deviation |
|---|---|---|
| Companies will act with high business standards | 3.44 | 0.498 |
| Companies have the skills and expertise | 3.75 | 0.435 |
| Companies are dependable | 3.27 | 0.445 |
| Companies do not have ill intensions | 3.21 | 0.412 |
| Companies are trustworthy | 3.21 | 0.412 |

### 4.3.6 Perceived Risk

Regarding risk perception, majority (about 84.6%) of the respondents believed that "providing credit card information over the web is unsafe" while only 15.3% of the respondents remained indifferent to the question. Moreover, majority (about 97.6%) of the respondents believed that "it would be risky to give personal information to online companies" while only 2.5% of the respondents remained indifferent to the question. Furthermore, majority (about 74.2%) of the respondents agreed that "there will be too much uncertainty associated with providing personal information" while the remaining 25.8% of the respondents remained neutral on this question.

Table 4.26
Responses on Perceived Risk

| Response | Credit Card Unsafe | | Risky for Info | | Uncertainty for Info | |
|---|---|---|---|---|---|---|
| | Freq. | % | Freq. | % | Freq. | % |
| St. disagree | 0 | 0 | 0 | 0 | 0 | 0 |
| Disagree | 0 | 0 | 0 | 0 | 0 | 0 |
| Neutral | 25 | 15.3 | 4 | 2.5 | 42 | 25.8 |
| Agree | 136 | 83.4 | 145 | 89.0 | 110 | 67.5 |
| St. agree | 2 | 1.2 | 14 | 8.6 | 11 | 6.7 |
| Total | 163 | 100 | 163 | 100 | 163 | 100 |

There was no significant difference between the mean score of the items related to risk perception, which ranged from 3.81 to 4.06. The standard deviations for the mean values ranged from 0.328 to 0.539. Among the three items, "risky to give information over web" had lowest standard deviation of 0.328 with mean of 4.06 and consumers' beliefs on "uncertainty for providing information over web" had highest standard deviation of 0.539 with mean value of 3.81, as shown in Table 4.27.

Table 4.27
Mean Value and Standard Deviation for the Items of Perceived Risk

| Items | Mean | Std. Deviation |
|---|---|---|
| Credit card info over Web is unsafe | 3.86 | 0.383 |

| | | |
|---|---|---|
| Risky to give info over Web | 4.06 | 0.328 |
| Uncertainty for providing info over Web | 3.81 | 0.539 |

### 4.3.7 Economic Incentives

Regarding economic incentives, about 47.2% of the respondents agreed that "providing credit card information over the web would not matter much if the prices are considerably lower" while only 1.2% of the respondents did not believe this. The remaining 51.5% of the respondents remained indifferent to the question. Furthermore, majority (about 80.4%) of the respondents agreed that "providing credit card information over the web would not matter much if the products/services are of a higher quality" and the remaining about 19.6% of the respondents remained neutral on this question, as shown in Table 4.28. There was no significant difference between the mean score of the items related to economic incentives, which were 3.46 and 3.83. The standard deviations for the mean values were 0.439 and 0.524.

### 4.3.8 Institutional Trust

Regarding institutional trust, about 46.0% of the respondents reported that "they will trust to open financial account with a bank" while the remaining (about 54.0%) of respondents were not sure about this. Moreover, almost all the respondents reported that "they will trust to open financial account with a major credit card company", as shown in Table 5.28 below. There was no significant difference between the mean score of the items related to institutional trust, which were 3.46 and 4.52. The standard deviations for the mean values were 0.500 and 0.501.

Table 4.28

Responses on Economic Incentives and Institutional Trust

| Response | Low Price | | Higher Quality | | Trust with Bank | | Credit Card Company | |
|---|---|---|---|---|---|---|---|---|
| | Freq. | % | Freq. | % | Freq. | % | Freq. | % |
| St. disagree | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Disagree | 2 | 1.2 | 0 | 0 | 0 | 0 | 0 | 0 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Neutral | 84 | 51.5 | 32 | 19.6 | 88 | 54.0 | 0 | 0 |
| Agree | 77 | 47.2 | 127 | 77.9 | 75 | 46.0 | 79 | 48.5 |
| St. agree | 0 | 0 | 4 | 2.5 | 0 | 0 | 84 | 51.5 |
| Total | 163 | 100 | 163 | 100 | 163 | 100 | 163 | 100 |

### 4.3.9 Consumers' Trust

Regarding about the use of more complex and advanced method, the majority (about 73.0%) of the respondents agreed 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" while about 27.0% of the respondents remained neutral on this question. On providing all necessary guarantees to increase consumers' confidence to adopt e-commerce, the majority (about 99.4%) of the respondents agreed that "their confidence to adopt e-commerce will increase when online vendors provide all necessary guarantees to ensure security and privacy of their personal information" while only 0.6% of respondents were not sure about this, as shown in Table 4.29. There was no significant difference between the mean score of the items related to consumers' trust, which were 3.74 and 4.30. The standard deviations for the mean values were 0.456 and 0.473.

Table 4.29
Responses on Consumers' Trust

| Response | Advanced Method | | Necessary Guaranties | |
|---|---|---|---|---|
| | Freq. | % | Freq. | % |
| St. disagree | 0 | 0 | 0 | 0 |
| Disagree | 0 | 0 | 0 | 0 |
| Neutral | 44 | 27.0 | 1 | 0.6 |
| Agree | 118 | 72.4 | 112 | 68.7 |
| St. agree | 1 | 0.6 | 50 | 30.7 |
| Total | 163 | 100 | 163 | 100 |

### 4.3.10 Reliability Analysis

Reliability analysis was performed to assess the reliability of the scale used to measure the variables of interest. Reliability assessment of the entire scale was first computed followed by the assessments of individual items supposed to measure the research constructs. The overall reliability assessment of the entire scale was observed to be with a Cronbach's alpha of 0.771**.** A second test was conducted to assess the degree to which the items on the scale measure the hypothesized research constructs.

A total of twenty five items measuring six constructs and one dependent variable were assessed for reliability. Five items measuring information security concerns has a cronbach's alpha of 0.738, six items measuring information privacy concerns has a cronbach's alpha of 0.772, five items measuring trustworthiness of web vendors has a cronbach's alpha of 0.778, three items measuring Risk Perception has a cronbach's alpha of 0.641, two items measuring economic incentive has a cronbach's alpha of 0.642, two items measuring institutional trust has a cronbach's alpha of 0.607, and two items measuring consumers' trust in e-commerce transactions has a cronbach's alpha of 0.642, as shown in Table 4.30.

Table 4.30
Reliability Analysis Results

| Items in the scale | Number of Items | Cronbach's Alpha |
|---|---|---|
| Information Security Concerns | 5 | 0.738 |
| Information Privacy Concerns | 6 | 0.772 |
| Trust Beliefs of Web Vendors | 5 | 0.778 |
| Risk Perception | 3 | 0.641 |
| Economic Incentives | 2 | 0.642 |
| Institutional Trust | 2 | 0.607 |
| Consumers' Trust | 2 | 0.642 |

### 4.3.11 Factor analysis

Factor analysis was conducted to identify the influential factors affecting consumers' trust in e-commerce adoption. Considering all the 25 items on security and privacy of consumer's personal information, trust and reliability of web vendors, consumer's perceived risk, economics incentive, and institutional trust, were analyzed using principal component analysis. "Total Variance Explained" showed the extent to which total variance of the observed variables was explained by each of the principal components. Initial factor extraction revealed seven components with an absolute magnitude of eigenvalue greater than 1.0.

As shown in Table 4.31, the first principal component, which related to the economic incentives, was the largest part of the total variance, had an eigenvalue of 6.326 amounted to 25.304% of the total variance. The second principal component, which related to the consumers' perceived privacy, had a variance of about 1.907 and accounted for a further 7.630% of the total variance. The third principal component was related to the trustworthiness of web vendors, which had an eigenvalue of 1.880 amounted to 7.521% of the total variance. The forth principal component, which related to the consumers' perceived security, had an eigenvalue of about 1.578 and accounted for 6.312% of the total variance. The fifth principal component, which related to the consumers' perceived risk, had a variance of about 1.448 and accounted for a further 5.791% of the total variance. The six principal component was related to the consumers' trust in e-commerce transactions, which had an eigenvalue of 1.189 amounted to 4.756% of the total variance. The seventh principal component, which related to the institutional trust, had an eigenvalue of about 1.034 and accounted for 4.136% of the total variance. In general, all the seven principal components together accounted for 61.449% of the total variance in the original 25 items.

Table 4.31
Total Variance Explained

| Component | Initial Eigenvalues | | |
|---|---|---|---|
| | Total | % of Variance | Cumulative % |

| | | | |
|---|---|---|---|
| 1 | 6.326 | 25.304 | 25.304 |
| 2 | 1.907 | 7.630 | 32.934 |
| 3 | 1.880 | 7.521 | 40.455 |
| 4 | 1.578 | 6.312 | 46.766 |
| 5 | 1.448 | 5.791 | 52.557 |
| 6 | 1.189 | 4.756 | 57.313 |
| 7 | 1.034 | 4.136 | 61.449 |

*Extraction Method: Principal Component Analysis.*

Most items loaded onto the extracted factors. However, some items that were conceptualized to measure the information security concerns, information privacy concerns and trustworthiness of web vendors, had factor loading lower than 0.50. Therefore, six items, namely, not hesitate to purchase for security issues, adequate control to ensure security, information will not be misused, later verify information, companies will act with high business standards, and companies have skills and expertise, were excluded from further analysis. Table 4.32 displayed factor extraction and factor loading.

Table 4.32
Factor Extraction and Factor Loading

| Items in the scale | Factor 1 | Factor 2 | Factor 3 | Factor 4 | Factor 5 | Factor 6 | Factor 7 |
|---|---|---|---|---|---|---|---|
| Safe providing Info<br>Intended recipient<br>Info not altered | | | | 0.772<br>0.673<br>0.763 | | | |
| Control over Info<br>Not reveal Info<br>Effective mechanism<br>Ensure Privacy | | 0.711<br>0.763<br>0.780<br>0.700 | | | | | |
| Dependable | | | 0.666 | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| No ill intension<br>Trustworthy | | | 0.881<br>0.879 | | | | |
| Card unsafe<br>Risky to give Info<br>Uncertainty | | | | | 0.518<br>0.683<br>0.737 | | |
| Trust with bank<br>Trust with company | | | | | | | 0.869<br>0.531 |
| Lower price<br>Higher quality | 0.671<br>0.728 | | | | | | |
| Advance Method<br>Guaranties | | | | | | 0.714<br>0.621 | |

### 4.3.12 Hypotheses Testing

Correlation analysis was performed to indicate both the strength and the direction of the relationship between independent and dependent variables. Pearson correlation coefficients were performed in order to determine the relationships between perceived security, perceived privacy, trustworthiness of web vendors and perceived risk with consumers' trust to adopt e-commerce. The results showed that there is a very low correlation ($r = 0.015$) existed between perceived security and consumers' trust in e-commerce adoption. This can be said that since consumers get familiar with the World Wide Web and with the emerging information technologies to safe and secure themselves in dealing with e-commerce transactions, their concerns on security issues are turning less significant matter from time to time.

However, a slight positive correlation ($r = 0.156$ with $p<0.05$) existed between perceived privacy and consumers' trust in e-commerce adoption. In addition, the construct of perceived privacy slightly manifested itself primarily through perceived security ($r = 0.280$, $p = 0.000$). A low correlation ($r = 0.140$, $p>0.05$) existed between trustworthiness of web vendor and consumers' trust in e-commerce adoption, which implies that trustworthiness of web vendor has no impact on consumers' trust in e-commerce adoption. However, the construct of perceived privacy slightly manifested itself primarily through trustworthiness of web vendors ($r = 0.356$, $p = 0.000$). The perceived risk has no impact on consumers' trust in e-commerce adoption ($r = -0.054$, $p>0.05$).

The results also showed that there was a fair negative correlation (r = -0.467, p = 0.000) existed between economic incentives and consumers' perceived risk, which implies that the increase in economic incentive reduces a consumers' perceived risk in online transaction. However, a low correlation (r = -0.107) between institutional trust and consumers' perceived risk existed, and which implies that the increase in institutional trust does not reduce a consumers' perceived risk in online transaction, as shown in Table 4.33.

Table 4.33
Results of E-Commerce Adoption Factors Correlation

| | Security | Privacy | Vendor | Risk | Econ | Institute | Trust |
|---|---|---|---|---|---|---|---|
| Security | 1.000 | | | | | | |
| Privacy | 0.280 | 1.000 | | | | | |
| Vendor | 0.382 | 0.356 | 1.000 | | | | |
| Risk | -0.235 | -0.360 | -0.325 | 1.000 | | | |
| Econ | 0.276 | 0.263 | 0.321 | -0.467 | 1.000 | | |
| Institute | 0.071 | 0.030 | 0.150 | -0.107 | 0.098 | 1.000 | |
| Trust | 0.015 | 0.156 | 0.140 | -0.054 | 0.143 | 0.099 | 1.000 |

It was observed that the effect of privacy concern on risk perception was higher than that of security concern. This may be because consumers get more experienced and sophisticated in dealing with the Internet, the security concerns which they could have had at the beginning are not reflected in their risk perceptions. Consumers may also have adopted protective measures on themselves to protect their own privacy online, such as providing incorrect personal information when dealing with web vendors. In contrast to security concerns, consumers' privacy concerns can not be transformed over time with Internet experience. It is likely that consumers' privacy concerns may be strengthened by becoming more aware of media exposure on privacy violations in the context of e-commerce. On the other hand, consumers' security concerns can be transformed over time with their Internet experience and more awareness. Since consumers are able to ease their security concerns to some extent by using protective measures such as installing and updating firewall, anti-spyware tools and so on, they may become more confident in transacting with e-commerce.

In addition, consumers would consider the trust beliefs they may have towards web vendors and their risk perceptions. Web vendors can develop trust beliefs in consumers by ensuring them of their dependableness and trustworthiness in performing electronic commerce transactions. Moreover, web vendors can also encourage consumers to do business with them by ensuring the protection of their sensitive personal information. The trust beliefs of web vendors were affected by security and privacy concerns where the effect of security concerns is higher. It was observed that both the security and privacy concerns have the direct effects on trustworthiness of web vendors. Information security is a very sensitive issue to many organizations and it is difficult to obtain information on security deployment of organization. Different types of business have different security requirements, thus the weight of security controls will be different. Security is a continuous process, which is ongoing within organization and its measures are extensively required for e-commerce applications of all manner, running on the Internet. Therefore, those organizations running on the Internet should encourage correct security decisions and by periodically assessing the performance of an information security system can prevent or reduce the damage of security incidents.

Regression analysis was conducted to study the relationship between the predictors of consumers' security and privacy concerns, trustworthiness of web vendors and risk perception with consumers' trust on e-commerce adoption. The results showed that perceived security was not statistically significant $t=0.186$, $p>0.05$, which means consumers' perceived security does not have influence on consumers' trust in e-commerce transaction.

The slight positive relationship between consumers' perceived privacy and their trust on e-commerce adoption means that consumers would like to transact online more if they believe that their sensitive personal information are adequately controlled in dealing with e-commerce transactions. The sample correlation coefficients is 0.17, indicating that only 2.4% of the variance for the consumers' trust on e-commerce adoption in the sample can be accounted for consumers' perceived privacy measures. Moreover, the regression model showed only 1.8% (Adjusted R Square = 0.018) of the consumers' trust on e-commerce adoption will be influenced by consumers' perceived privacy. Trustworthiness of web vendors and risk perception do not have

influence on consumers' trust on e-commerce adoption, p>0.05. The sample correlation coefficients for trustworthiness of web vendors is 0.14, indicating that only 2% of the variance for the consumers' trust on e-commerce adoption in the sample can be accounted for trustworthiness of web vendors measures. In addition, the regression model showed only 1.3% (Adjusted R Square = 0.013) of the consumers' trust on e-commerce adoption will be influenced by trustworthiness of web vendors.

The regression analysis of the study showed that only one predictor (perceived privacy) out of four predictors was found to be slightly significant ($p < 0.05$) to the consumers' trust on e-commerce adoption. In overall, the regression model showed only 1.2% (Adjusted R Square = 0.012) of the consumers' trust on e-commerce adoption will be influenced by the consumers' security and privacy concerns, trustworthiness of web vendors and risk perception, as shown in Table 4.34.

Table 4.34
Regression Analysis Results

| Construct | Standard Coefficients Beta | t-value | Sig. |
|---|---|---|---|
| • Perceived security | 0.015 | 0.186 | 0.852 |
| • Perceived privacy | 0.156 | 2.005 | 0.047 |
| • Trustworthiness of web vendors | 0.140 | 1.792 | 0.075 |
| • Risk perception | 0.054 | 0.684 | 0.495 |

Dependent Variable: Consumers' Trust in e-commerce transactions

A multiple regression analysis was conducted to evaluate the relationship between the predictors of economic incentives and institutional trust with consumers' perceived risk. Table 4.35(i) through Table 4.35(iii) presented the results of multiple regression analysis computed for risk as dependent variable and the two predictors which are economic incentives and institutional trust.

The linear combination of the economic incentives and institutional trust was significantly related to the consumers' perceived risk $F(2, 160) = 22.827$, $p<0.01$ as shown in Table 4.35(ii). The results showed that the increase on economic incentives and institutional trust will reduce consumers' perceived risk. The sample multiple correlation coefficients is 0.471, indicating that about 22.2% of the variance for the

consumers' perceived risk in the sample can be accounted for by the linear combination of economic incentives and institutional trust measures.

The regression analysis of this study showed that only economic incentives predictor was found to be significant to the consumers' perceived risk. In overall, the regression model showed approximately 21.2% (Adjusted R Square = 0.212) of the consumers' perceived risk will be influenced by economic incentives and institutional trust.

Table 4.35(i)
Regression Model Summary

| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate |
|---|---|---|---|---|
| 1 | 0.471 | 0.222 | 0.212 | 0.28868 |

Predictors: (Constant), Economic incentives, Institutional trust
Dependent Variable: Consumers' perceived risk

Table 4.35(ii)
ANOVA

| Model | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| 1 | Regression | 3.805 | 2 | 1.902 | 22.827 | 0.000 |
| | Residual | 13.334 | 160 | 0.083 | | |
| | Total | 17.138 | 162 | | | |

Predictors: (Constant), Economic incentives, Institutional trust
Dependent Variable: Consumers' perceived risk

Table 4.35(iii)
Predictors Coefficients

| | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
|---|---|---|---|---|---|
| | B | Std. Error | Beta | | |
| (Constant) | 5.437 | 0.295 | | 18.418 | 0.000 |
| Economic incentives | -0.362 | 0.055 | -0.461 | -6.579 | 0.000 |
| Institutional trust | -0.052 | 0.059 | -0.062 | -0.885 | 0.378 |

Dependent Variable: Consumers' perceived risk

**H1:** A consumer's perceived security of online transaction positively influences his/her trust in online transaction.

The result of the study showed that perceived security does not affect the consumers' trust in e-commerce adoption. The correlation coefficient between consumers' perceived security towards online transaction and their confidence to adopt e-commerce was found to be with ($r = 0.015$, $p>0.05$). Therefore, the research hypothesis was not supported.

**H2:** A consumer's perceived privacy of online transaction positively influences his/her trust in online transaction.

The result of the study showed that perceived privacy slightly influences the consumers' trust in e-commerce adoption. The relationship was observed to be with ($r = 0.156$, $p < 0.05$). Therefore, the research hypothesis was supported.

**H3:** A consumer's perceived privacy of online transaction positively influences perceived security of online transaction.

The result of the study showed that consumer's perceived privacy of online transaction on trust was mediated by perceived security ($r = 0.280$). The relationship was observed to be statistically significant with significance level less than 0.01 ($p = 0.000$). Therefore, the research hypothesis was supported.

**H4:** The trustworthiness of web vendor positively influences a consumer's trust in online transaction.

The results of the study showed that trustworthiness of web vendor did not influence the consumers' trust in e-commerce adoption. The relationship was observed to be insignificant ($r = 0.140$, $p > 0.05$). Therefore, the research hypothesis was not supported.

**H5:** A consumer's perceived privacy of online transaction positively influences the trustworthiness of web vendor of online transaction.

The result of the study showed that consumer's perceived privacy of online transaction on trust was mediated by trustworthiness of web vendor ($r = 0.356$). The relationship was observed to be statistically significant with significance level less than 0.01 ($p = 0.000$). Therefore, the research hypothesis was supported.

**H6:** A consumer's perceived risk in online transaction positively influences his/her trust in online transaction.

The results of the study showed that a consumer's perceived risk in online transaction did not influence his/her trust in online transaction ($r = -0.054$, $p > 0.05$). Therefore, the research hypothesis was not supported.

**H7:** The increase in economic incentives reduces consumers' perceived risk in online transaction.

We found that the increase in economic incentives reduced a consumers' perceived risk in online transaction. The relationship was observed to be statistically significant ($r = -0.467$, $p < 0.01$). Therefore, the research hypothesis was supported.

**H8:** The increase in institutional trust reduces consumers' perceived risk in online transaction.

We found that the increase in institutional trust did not reduce a consumers' perceived risk in online transaction. The relationship was observed to be with ($r = -0.107$, $p > 0.05$). Therefore, the research hypothesis was not supported.

### 4.4 Overall Study

#### 4.4.1 Sample Demographics

Overall, two hundred and forty eight respondents (58.1% males and 41.9% females) were participated for the purpose of analysis for this study. The majority of the respondents (about 87.1%) were age between 20 to 30, followed by age between 31 to 40 (about 12.1%) and while remaining about 0.8% were age between 41 to 50. The results showed that the sample was skewed towards age between 20 to 30, with the mean of 1.14 and standard deviation of 0.367. In term of races, about 55.2% were Malay, followed by Chinese race (about 21.8%), while about 13.7% were Indian and about 9.3% were other races, as shown in Table 4.36.

Table 4.36
Overall Respondents' Demographic Information and E-commerce Issues

| Variables | Frequency | Percent |
|---|---|---|
| Gender | | |
| • Male | 144 | 58.1 |
| • Female | 104 | 41.9 |
| Age group | | |
| • 20 -30 years | 216 | 87.1 |
| • 31-40 years | 30 | 12.1 |
| • 41-50 years | 2 | 1.2 |
| • 51 years and above | 0 | 0 |
| Race | | |
| • Malay | 137 | 55.2 |
| • Chinese | 54 | 21.8 |
| • Indian | 34 | 13.7 |
| • Others | 23 | 9.3 |
| Internet Usage | | |
| • Always | 231 | 93.1 |
| • Sometimes | 14 | 5.6 |
| • Seldom | 3 | 1.2 |
| • Never | 0 | 0 |
| Credit card security | | |
| • Very unsafe | 22 | 8.9 |
| • Somewhat unsafe | 60 | 24.2 |
| • Indifferent | 32 | 12.9 |
| • Somewhat safe | 108 | 43.5 |
| • Very safe | 5 | 2.0 |
| • Don't know | 21 | 8.5 |

Out of the 248 overall respondents, almost all the respondents (about 93.1%) reported that "they frequently use the internet" while about 5.6% reported that "they sometimes use the internet". The remaining 1.2% reported that "they seldom use the internet". All the respondents were also asked about their opinions on credit card security for online purchases. The majority of the respondents (about 43.5%) believed that "the use of credit card for online purchases is somewhat safe" while about 22.2% believed "somewhat unsafe". About 12.9% of the respondents were indifferent on online credit card security while about 8.9% believed "very unsafe". About 8.5% of the respondents were not sure about this while the remaining (about 2.0%) respondents believed "very safe".

### 4.4.2 Reliability Analysis

Reliability analysis was performed to assess the reliability of the scale used to measure the variables of interest. Reliability assessment of the entire scale was first computed followed by the assessments of individual items supposed to measure the research constructs. The overall reliability assessment of the entire scale was observed to be with a Cronbach's alpha of 0.876**.** A second test was conducted to assess the degree to which the items on the scale measure the hypothesized research constructs.

A total of twenty five items measuring six constructs and one dependent variable were assessed for reliability. Five items measuring information security concerns had a cronbach's alpha of 0.818, six items measuring information privacy concerns had a cronbach's alpha of 0.701, five items measuring trustworthiness of web vendors had a cronbach's alpha of 0.715, three items measuring risk perception had a cronbach's alpha of 0.707, two items measuring economic incentive had a cronbach's alpha of 0.616, two items measuring institutional trust had a cronbach's alpha of 0.768, and two items measuring consumers' trust in e-commerce transactions had a cronbach's alpha of 0.758, as shown in Table 4.37.

Table 4.37
Reliability Analysis Results

| Variables in the Scale | Number of Items | Cronbach's Alpha |
|---|---|---|
| Perceived Information Security | 5 | 0.818 |
| Perceived Information Privacy | 6 | 0.701 |
| Trustworthiness of Web Vendors | 5 | 0.715 |
| Perceived Risk | 3 | 0.707 |
| Economic Incentives | 2 | 0.616 |
| Institutional trust | 2 | 0.768 |
| Consumers' Trust | 2 | 0.758 |

### 4.4.3 Structural Equation Modeling (SEM)

Structural Equation Modeling (SEM) requires two procedural steps. The measurement model was tested by Confirmatory Factor Analysis (CFA) and then the fit of the full research model was assessed. Both the measurement model fit and the full research model fit were examined by calculating the chi-square value. Given the known sensitivity to the sample size (n>200, Bagozzi and Yi, 1988), chi-square/df was also used to determine the fit of the research model. This study applied several model fit indices such as Root Mean Square Error of Approximation (RMSEA, <.05 is good and <.08 is acceptable), Goodness of Fit Index (GFI, > 0.90 is good), Normed Fit Index (NFI, > 0.90 is acceptable), and Comparative Fit Index (CFI, >.90 is acceptable). When there is supporting evidence of the research model acceptance, the parameter estimates were examined. Parameter estimates are admissible when the correlations of estimates are not bigger than 1.00, no variance is negative, covariance or correlation matrices are positively defined, and standard errors are not excessively small (too close to 0) or large (too close to 1).

### 4.4.4 Confirmatory Factor Analysis

Confirmatory Factor Analysis (CFA) was conducted to assess the measurement model. Originally, seven latent variables and a total of 25 indicators were used to conduct CFA. For the perceived information security factor, the resulting chi-square statistic for the initial five indicators (chi-square = 19.313; df = 5; p = 0.002, chi-square/df = 3.863) and other indications showed that the measurement model factor did not fit quite well to the data (GFI = 0.968; AGFI = 0.905; CFI = 0.964, NFI = 0.953; RMSEA = .108). The poor fit of the model factor can be revised by investigating modification indices or the standard residuals (Hair et al., 1998). In order to improve the model factor, indicators which were related to problematic standard residuals (2.5 as a cut-off) or larger reductions of chi-square were identified and eliminated one by one. After removing an indicator (the information is not altered in transit), an acceptable model factor was achieved (chi-square = 4.394; df = 2; p = 0.111; chi-square/df = 2.197 <3; GFI = 0.991; AGFI = 0.954; CFI = 0.992, NFI = 0.985; RMSEA = .07).

While assessing the perceived information privacy factor, the resulting chi-square statistic for the initial six indicators (chi-square = 36.899; df = 9; p = 0.000, chi-square/df = 4.1) and other indications showed that the measurement model factor did not fit quite well to the data (GFI = 0.954; AGFI = 0.892; CFI = 0.895; NFI = 0.869; RMSEA = .112). After removing an indicator (online companies will not reveal sensitive information), an acceptable model factor was achieved (chi-square = 8.356; df = 5; p = 0.138; chi-square/df = 1.671<3; GFI = 0.987; AGFI = 0.960; CFI = 0.984; NFI = 0.962; RMSEA = 0.052).

The resulting chi-square statistic for the trustworthiness of the web vendors model factor with the initial five indicators (chi-square = 18.386; df = 5; p = 0.002, chi-square/df = 3.677) and other indications showed that the measurement model factor did not fit quite well to the data (GFI = 0.969; AGFI = 0.906; CFI = 0.944; NFI = 0.926; RMSEA = 0.104). After removing an indicator (online companies are dependable), an acceptable model factor was achieved (chi-square = 4.308; df = 2; p = 0.116; chi-square/df = 2.154<3; GFI = 0.991; AGFI = 0.957; CFI = 0.986; NFI = 0.975; RMSEA = 0.068). For the remaining four factors, namely, perceived risk, economic incentives, institutional trust, and consumers' trust; chi-square statistic and other indications could not be conducted to assess the measurement model factor due to the numbers of item included, i.e. less than 4 items. Thus, these four factors were considered as acceptable model factors.

### 4.4.5 Overall Model Fit

The assessment of the overall model fit was to test the hypothesized relationships in a research model. This analysis was conducted with seven latent variables and 22 indicators defined from the Confirmatory Factor Analysis (CFA) in the prior procedure.

The initially hypothesized model was not accepted as shown in Table 5.38. The chi-square was significant (chi-square = 561.597; df = 201, p=0.002, chi-square/df = 2.794<3) and the model fit indices did not strongly support the fit of the overall model (GFI = 0.826; AGFI = 0.781; CFI = 0.809; NFI = 0.735; RMSEA = 0.085). Hair et al. (1998) stated that the poor fit of the overall model could be revised by investigating

modification indices or the standard residuals. Moreover, as suggested by Anderson and Gerbing (1988), in order to improve the model factor, indicators which were related to problematic standard residuals (2.5 as a cut-off) or larger reductions of chi-square were identified and eliminated one by one.

Table 4.38 presented the eliminated indicators in each run and the evidence of the overall model fit. An indicator dropped at first was from a variable of perceived information privacy (control over how the information provided will be used by online companies). Next, the dropped indicator was (online companies do not have ill intentions about any of their consumers) from a variable of trustworthiness of the web vendors, followed by (online companies are trustworthy) from a variable of trustworthiness of the web vendors, (information would not be misused when transacting with online companies) from a variable of perceived information privacy, (totally safe providing information over the Web) from a variable of perceived information security, (risky to give information to online companies) from a variable of perceived risk, (there is an effective mechanism to address any violation of the sensitive information) from a variable of perceived risk, and (the payment information is safe and accessible only by the intended recipient) from a variable of perceived information security.

Table 4.38
Overall Model Fit and the Revisions with Eliminated Items

| SEM | Eliminated Item | Evidence of the Model Fit |
|---|---|---|
| 1st | None<br>(Run: 7 latent variables with 22 indicators) | • chi-square = 561.597; df = 201; p = 0.002, chi-square/df = 2.794 <3<br>• GFI = 0.826; AGFI = 0.781; CFI = 0.809; NFI = 0.735; RMSEA = 0.085 |
| 2nd | Control over how the information provided will be used<br>(Run: 7 latent variables with 21 indicators) | • chi-square = 519.733; df = 181; p = 0.011, chi-square/df = 2.871 <3<br>• GFI = 0.832; AGFI = 0.785; CFI = 0.818; NFI = 0.749; RMSEA = 0.087 |
| 3rd | Online companies do not have ill intentions | • chi-square = 468.317; df = 162; p = 0.016, chi-square/df = 2.891 <3 |

| | | |
|---|---|---|
| | (Run: 7 latent variables with 20 indicators) | • GFI = 0.839; AGFI = 0.791; CFI = 0.830; NFI = 0.765; RMSEA = 0.087 |
| 4th | Online companies are trustworthy (Run: 7 latent variables with 19 indicators) | • chi-square = 414.203; df = 144; p = 0.038, chi-square/df = 2.876 <3<br>• GFI = 0.846; AGFI = 0.797; CFI = 0.844; NFI = 0.783; RMSEA = 0.087 |
| 5th | Information would not be misused (Run: 7 latent variables with 18 indicators) | • chi-square = 377.751; df = 127; p = 0.039, chi-square/df = 2.974 <3<br>• GFI = 0.854; AGFI = 0.803; CFI = 0.849; NFI = 0.792; RMSEA = 0.089 |
| 6th | Totally safe providing information over the Web (Run: 7 latent variables with 17 indicators) | • chi-square = 326.606; df = 111; p = 0.041, chi-square/df = 2.942 <3<br>• GFI = 0.869; AGFI = 0.820; CFI = 0.858; NFI = 0.803; RMSEA = 0.089 |
| 7th | Risky to give information to online companies (Run: 7 latent variables with 16 indicators) | • chi-square = 283.468; df = 96; p = 0.043, chi-square/df = 2.953 <3<br>• GFI = 0.879; AGFI = 0.828; CFI = 0.867; NFI = 0.815; RMSEA = 0.089 |
| 8th | Information is safe and accessible only by the intended recipient (Run: 7 latent variables with 15 indicators) | • chi-square = 236.849; df = 82; p = 0.049, chi-square/df = 2.888 <3<br>• GFI = 0.892; AGFI = 0.843; CFI = 0.878; NFI = 0.827; RMSEA = 0.087 |

Two possible paths suggested by the modification indices were paths from Institutional Trust to Perceived Information Privacy and from Economic Incentives to Perceived Information Privacy. Firstly, the model was revised by adding a path from Institutional Trust to Perceived Information Privacy. The chi-square was significant (chi-square =202.103; df = 81, p = 0.053, chi-square/df=2.495<3) and the model fit indices support the fit of the overall model (GFI = 0.904; AGFI=0.858; CFI = 0.904; NFI = 0.853; RMSEA = 0.078). The modification indices were investigated again, and another path was added to the model. By including a path from Economic Incentives to Perceived Information Privacy, RMSEA was dropped to .069 and the model was accepted (chi-square = 173.701; df = 80; p = 0.059, chi-square/df = 2.171 <3, GFI = 0.914; AGFI = 0.870; CFI = 0.926; NFI = 0.873; RMSEA = .069) as shown in Table 4.39. The parameter estimates were admissible and there were no negative variances.

Table 4.39
Overall Model Fit and the Revisions with Added Paths

| SEM | Added Path | Evidence of the Model Fit |
|---|---|---|
| 1st | Institutional Trust → Perceived Information Privacy | • chi-square = 202.103; df = 81; p = 0.053, chi-square/df = 2.495 <3<br>• GFI = 0.904; AGFI = 0.858; CFI = 0.904; NFI = 0.853; RMSEA = 0.078 |
| 2nd | Economic Incentives → Perceived Information Privacy | • chi-square = 173.701; df = 80; p = 0.059, chi-square/df = 2.171 <3<br>• GFI = 0.914; AGFI = 0.870; CFI = 0.926; NFI = 0.873; RMSEA = 0.069 |

Standardized path coefficients and significance were presented in Table 4.40 and Figure 4.5. The hypotheses (H1, H2, H4 and H6) were developed to test the importance of perceived information security, perceived information privacy, trustworthiness of the web vendors, and perceived risk to explain the consumers' trust in e-commerce transactions. An insignificant positive relationship was found in a path from perceived information security to consumers' trust (H1). Moreover, perceived information privacy and trustworthiness of the web vendors did not significantly affect consumers' trust (H2 and H4). However, a path from perceived risk to consumers' trust (H6) was significant (0.51).

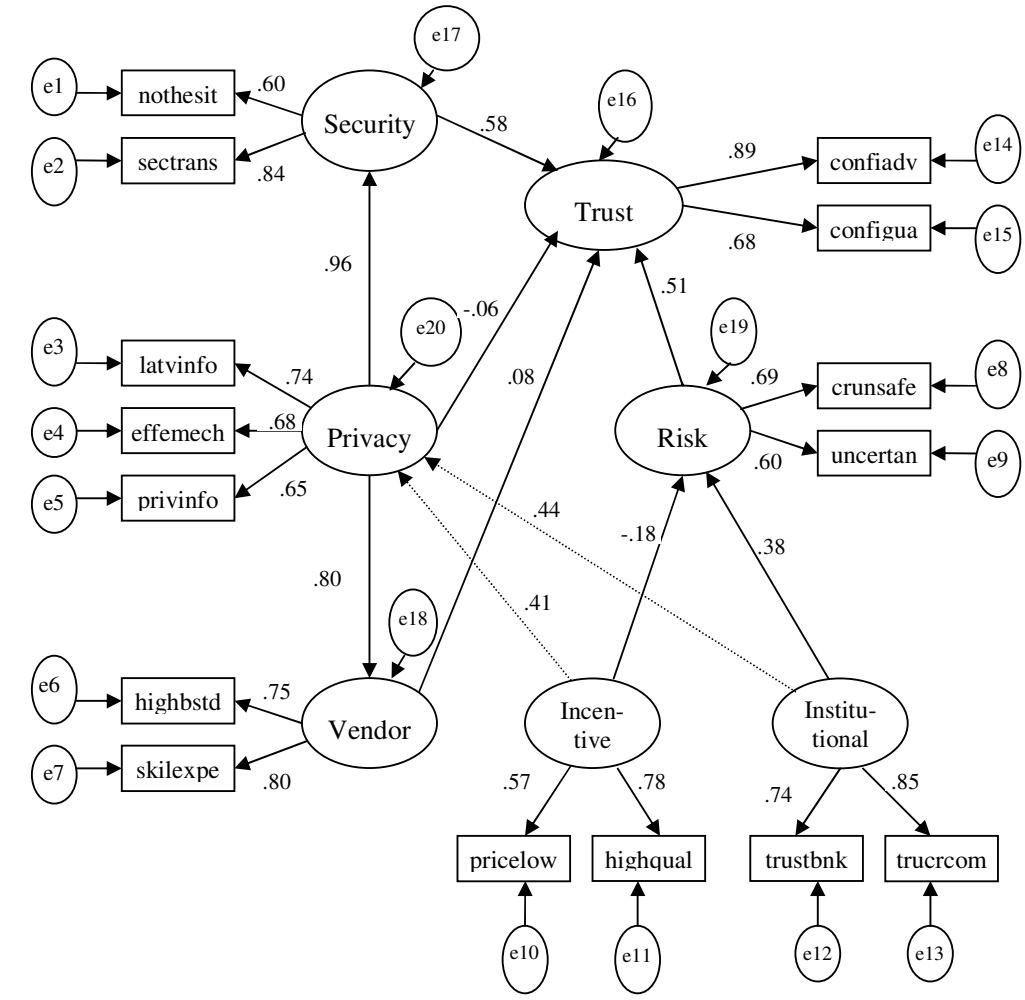
A strong influence of perceived information privacy on perceived information security (H3) was identified (0.96), and the path from perceived information privacy to trustworthiness of the web vendors (H5) was significant (0.80). The hypotheses (H7 and H8) were proposed to study the role of institutional trust and economic incentives in consumers' perceived risk. The influence of institutional trust on consumers' perceived risk (H8) was significant (0.38), but economic incentives did not significantly affect consumers' perceived risk (H7).

Finally, the revised model included two additional paths, a path from institutional trust to consumers' perceived privacy and from economic incentives to consumers' perceived privacy, and both relationships were positively significant (0.44 and 0.41).

Squared multiple correlations indicate the extent of explained portions of endogenous variables. The highest percentage appeared in perceived information privacy (91 %), and the next highest percentages were shown in consumers' trust (65 %) and trustworthiness of the web vendors (64 %). Compared with the percentages of explained portions of those variables, those percentages of perceived information privacy (36%) and perceived risk (17 %) were lower.

Table 4.40
Standardized Path Coefficients

| Outcome | Determinant | Hypothesis | Coefficients |
|---|---|---|---|
| Consumers' Trust ($R^2 = 0.65$) | Security | H1 | 0.58 |
| | Privacy | H2 | -0.06 |
| | Vendor | H4 | 0.08 |
| | Risk | H6 | 0.51** |
| Perceived Information Security ($R^2 = 0.91$) | Privacy | H3 | 0.96** |
| Trustworthiness of the Web Vendors ($R^2 = 0.64$) | Privacy | H5 | 0.80** |
| Perceived Risk ($R^2 = 0.17$) | Incentives | H7 | -0.18 |
| | Institute | H8 | 0.38** |
| Perceived Information Privacy ($R^2 = 0.36$) | Institute | H9 | 0.44** |
| | Incentives | H10 | 0.41** |




Security: Perceived Information Security

Privacy: Perceived Information Privacy

Vendor: Trustworthiness of Web Vendors

Risk: Perceived Risk

Incentive: Economic Incentives

Institutional: Institutional Trust

Figure 4.5. Finalized Research Model Fit.

Table 4.41 showed the standardized loadings of each indicator and Cronbach's alpha for the latent variables for the final proposed model. Path coefficients from latent variables to their corresponding indicators were high (between 0.59 and 0.89) and all loadings were significant ($p<0.05$). Since ten indicators were deleted,

Cronbach's alpha was assessed again and the resulting values ranged between 0.601 and 0.768.

Table 4.41
Standardized Loadings of Indicators to the Corresponding Variables

| Constructors & Indicators | Standardized Loadings | Cronbach's Alpha |
|---|---|---|
| Perceived Information Security | | 0.663 |
| • nothesit | 0.60 | |
| • sectrans | 0.84 | |
| Perceived Information Privacy | | 0.746 |
| • latvinfo | 0.74 | |
| • effemech | 0.68 | |
| • privinfo | 0.65 | |
| Trustworthiness of Web Vendors | | 0.751 |
| • highbstd | 0.75 | |
| • skilexpe | 0.80 | |
| Perceived Risk | | 0.601 |
| • crunsafe | 0.69 | |
| • uncertain | 0.60 | |
| Economic Incentives | | 0.616 |
| • pricelow | 0.57 | |
| • highqual | 0.78 | |
| Institutional Trust | | 0.768 |
| • trustbnk | 0.74 | |
| • trucrcom | 0.85 | |
| Consumers' Trust | | 0.758 |
| • confiadv | 0.89 | |
| • configua | 0.68 | |

Overall, regarding online information security concerns, the majority respondents (about 44.8%) agreed that "they will not hesitate to make purchase from the web because of security issues of sensitive information" and also majority (about 66.5%) of the respondents believed that "there is an adequate control in place to ensure security of personal data transmitted during online transaction processing". On the subject of online information privacy concerns, majority (about 71.4%) of the respondents believed that "they can later verify the information they provide to online

companies" while majority (about 51.6%) of the respondents believed that "there is an effective mechanism to address any violation of the sensitive personal information they provide to online companies" and also majority (about 66.5%) of the respondents believed that "there is an adequate control in place to protect the privacy of sensitive personal information". Concerning the trustworthiness of web vendors, majority (about 49.6%) of the respondents believed that "online companies will act with high business standards" while majority (about 67.3%) of the respondents believed that "online companies have the skills and expertise to perform transactions in an expected manner".

Regarding risk perception, majority (about 66.9%) of the respondents believed that "providing credit card information over the web is unsafe" and majority (about 73.4%) of the respondents agreed that "there would be too much uncertainty associated with providing personal information to online companies". Concerning economic incentives, majority (about 72.6%) of the respondents agreed that "providing credit card information over the web will not matter much if the prices are considerably lower" and majority (about 71.7%) of the respondents agreed that "providing credit card information over the web will not matter much if the products or services are of a higher quality". Concerning institutional trust, majority (about 68.9%) of the respondents would trust to open financial account with a Bank, and majority (about 88.7%) of the respondents would trust to open financial account with a major credit card company.

On the subject of consumers' trust, the majority (about 87.9%) of the respondents agreed that "their confidence to purchase online will be increased when more complex and advanced method is used to address the concerns on their security and privacy" while the majority (about 81.1%) of the respondents agreed that "their confidence to adopt e-commerce will increase when online vendors provide all necessary guarantees to ensure security and privacy of their sensitive personal information".

## 4.5 Chapter Summary

Following the discussion on our research methodology and theoretical framework, this chapter initially concentrated on the conduct of the survey data analysis. We started with the internet savvy final year undergraduate students from the two universities in which the initial study took place. The purpose of conducting this initial study was to explore the possibility of students' willingness to make online purchases in the near future and their perceptions on security and privacy issues, trust and reliability of web vendors, and risk perceptions as they pertain to adopt e-commerce. Our findings suggested that trustworthiness of web vendors and perceived risk influence non-online purchasers' trust on e-commerce adoption.

The second study was focused on the general public online consumers in order to explore their perceptions on e-commerce transactions related to perceived information security, perceived information privacy, trustworthiness of web vendors and perceived risk. The results showed that online consumers do perceive privacy of their sensitive personal information in dealing with e-commerce transactions.

Overall findings suggested that consumers' perceived risk influences their trust in e-commerce transactions. The construct of perceived privacy manifests itself primarily through perceived security as well as trustworthiness of web vendors. In addition, the institutional trust influences a consumers' perceived risk in online transaction. The findings also suggested that economic incentives and institutional trust have relationships or associations with consumers' perceived privacy.

In addition to the findings related to our survey data analysis, semi-structured interviews gave us additional information concerning both the use of the online transaction system in general and other consequences. The next chapter concentrates on further discussion of our findings in relation to interviewees' perceptions in dealing with e-commerce transactions.

# CHAPTER 5

# INTERVIEW FINDINGS

## 5.1 Introduction

While the previous chapter of this study presented the empirical findings and analysis of the variables of interests, this chapter provides the interpretation of the interviewees' perspectives. The first section of this chapter provides a brief explanation of the reason and procedures for conducting semi-structured theme interview followed by the detail explanation of the interview findings based on study constructs.

## 5.2 Interviewees' Perspectives

In order to know more about consumers' views on their perceptions related to e-commerce transactions, we planned to link up a qualitative method, i.e., a semi-structured based interview, with a quantitative survey method. In addition, we decided to include a semi-structured theme interview is affirmed by the concept that a qualitative method is helpful in a condition where a wealthy amount of data is required to create possibilities to realize the phenomenon as largely as possible and to produce new insights.

The collection of the data for the analysis was made during the early of 2010. Fifteen interviewees were participated, six of them were male and nine were female. Seven were below 30 years old and eight were between 30–40 years. The interviewees were recruited by referral samples. The interviewees had diverse experiences and backgrounds in dealing with e-commerce transactions. The length of

the interviews took from 45 minutes to one and half hours. The interviews were carried out in the interviewees' working places, over online and homes. Firstly, the participants were asked about general backgrounds in dealing with e-commerce transactions and then discussed about their perceptions on information security and privacy, trustworthiness of web vendors and risk related to e-commerce transactions. All of the interviewees' responses were noted and completely transcribed, and the discussions of the findings were presented based on study constructs. With the intention of clarifying the concepts from consumers' viewpoints, we compared our results from surveyed studies with literature and the interviewees' perceptions.

### 5.2.1 Perceived Information Security

In e-commerce environment, commercial transactions could be regarded as secure, if the required information comes from the correct entities and arrives at the expected parties without being viewed, changed, interrupted or damaged by inappropriate parties during transit and being stored at web vendors' computers. The emerging of new information technologies has always been come with the concerns on security, and thus, the growth and development of e-commerce require to control information security threats, by improving consumers' security and privacy perceptions and building trust with web vendors. Certainly, the implementation of providing a successful e-commerce is not an easy charge. Several issues need to be taken into consideration, such as security and privacy of consumers' sensitive personal information during online transactions as well as within online companies. Many researchers (Pavlou and Chellappa, 2001; Belanger et al., 2002; Ahuja et al., 2003; Kai et al., 2004; Laforet and Li, 2005 and Ahmed et al., 2007) found that security and privacy concerns were the single biggest barriers to online commerce.

Security and privacy breach in online companies' servers can influence any individual that online thieves are hanging around to steal consumers' sensitive personal information in dealing with e-commerce transactions. However, today Internet security expert will believe, providing consumers' sensitive personal information to reputable online store site is, in fact, much more secure compare to providing their credit card information to real-world commerce. Today, Internet security experts believe that when consumer provides a credit card number and other

sensitive personal information to a well-known online store site, he or she is transferring it over a secure connection to legitimate web vendor and saved from even the most strong-minded intruders over the Internet. However, security breaches can be faced since small online store sites frequently outsource their computing systems for e-commerce, and some web vendors do not recognize or concern about secure e-commerce technologies. One of the interviewees responded that:

> "I have not been troubled with security threats, though I have heard a number of security breaches on media. Sometimes, we find broken link and cannot do transaction. There are also like we may receive email from somebody we don't know. Our computers can be affected by viruses since they can come to our mail as confidential document files. Sometimes, we have problem with logging into e-services. But, I don't think these kinds of things can be considered as security threats."

The above quotation illustrates how consumer's concern on security issues do not influence her trust in e-commerce transactions regarding perceived risks. Moreover, the difficulty to access the desired online store site due to failure of the information technology can not be understood as increasing consumers' perceived risks in dealing with e-commerce transactions. The security threat like accessibility problem can not have an influence on consumers' trust towards online transactions, for the reason that disappointed experiences associated with the functions of online store site' services may not normally reduce the consumers' trust to participate in e-commerce transactions.

Since the Internet is open and borderless medium for communicating and sharing research information, it was not programmed with security features and also it was not intended for sensitive commercial use. There have always been growing numbers of attack on commercial networking environment due to the increasing in e-commerce activities. For that reason, it is now generally agreed that e-commerce transactions would be highly susceptible to security threats without adequate control mechanisms.

Even if today consumers do not perceive more on information security, web vendors should clearly assess the effectiveness of security mechanisms for their online store sites since these are apparently expensive technological investments to

gain successful business in competitive environment over the web. The interviewee noted about an unsecured transaction by saying that:

> "I noticed the goods I was searching for at a cheaper cost to give as a present to my friend. I decided to buy it anyways though I didn't have experienced with that store site. However, when I went to look into, a warning sign appeared and I neglected the store site right away. It was not worth though it's a great price; there was a problem with the security certificate of that store site and I might get in trouble in dealing with that store site. By this way, we can prevent from any security threats."

In the perspective of e-commerce transactions, security threats can be identified at beginning of transaction, throughout transit, and at being stored in web vendors' computing systems. Moreover, security breaches might be categorized based on how the consumers' sensitive personal information is involved, i.e., loss of integrity, confidentiality and availability. Security threats may also be categorized based on how the involved parties are presented in dealing with e-commerce transactions, i.e., authorization, verification, and non-repudiation. However, these are mainly indicators for the evaluation of security threats by Information systems professionals and thus, how consumers' perceived security of their sensitive personal information may be different. Mustafa and Mohd Khairuddin (2003) and Yusof and Mohd Yusof (2005) suggested that the need for security and reliability as the major concern barriers to e-commerce adoption in Malaysia.

Some of the interviewees concern confidentiality as problem mainly due to their risk concerns on interrupting their sensitive personal information in dealing with e-commerce transactions. The interviewee's thought revealed that:

> "I prefer to use online banking systems. It is really convenient to use at online store sites operated in own country. However, there are well-known online store sites across the border, but I would not purchase from foreign online stores because I have to deal with my credit card number and I do not really want to take the risk of facing security threats."

The interviewee's thought can be revealed reflection of the connection between her concerns on security and in turn, it leads to her perceived risks in order to transact with web vendors across the border. She will be more confident to deal with web vendors from her own country only rather than foreign online stores by believing that web vendors from own country will handle security related issues more efficiently compared to foreign online stores. However, another interviewee stated that:

> "I often order books from Thailand based online stores because it is much cheaper and I don't face any security breaches. I believe, if we purchase from well-known vendors abroad and also no security warnings pop-up when dealing with unknown web vendors, there won't be any problem to participate in e-commerce transactions. It's really convenient and can get much cheaper price."

The consumers' perceptions of security are generated in the course of encryption process, such as, an unreadable key, process of protection such as statements about information protection and firewalls, process of verification such as familiar and verifiable domain names, process of authentication such as digital certificates from trusted third parties. Therefore, even though web vendors carry out the scientific measurement of security with the use of emerging information technological solutions, it is consumers' perceptions of security that could power trust in dealing with e-commerce transactions.

### 5.2.2 Perceived Information Privacy

In dealing with e-commerce transactions, privacy touches on parts of being gathered and stored, and distribution of consumers' sensitive personal information for unintended purposes. Due to the capability of the emerging information technologies for the criminal activities, consumers' concerns on privacy of their sensitive personal information become the ever more essential issue. As a result, consumes' distrustfulness is rising, concerning on how their sensitive personal information is obtained, stored and handled. Privacy concern was discovered as a most important barrier to e-commerce adoption (Malhotra et al., 2004).

Online consumers will not be getting sufficient safety, in Malaysia, until the Malaysian government takes steps to modify some of the present laws to deal with the issues in e-commerce sufficiently (Jawahitha, 2004). The below citation shows the consumers' concerns on privacy issues relates to their sensitive personal information, in general, which will be used for unintended purposes, such as, direct advertising, distribution of the sensitive personal information without the permissions of the consumers. The interviewee noted that:

> "In dealing with less-known web vendors, I concern how my provided information will be handled. I also concern whether I will be informed to use my information for other unintended purposes or share with other companies for direct marketing purposes. But until now, I don't face any privacy breaches."

It is clear to say that online consumers are slightly concerned about their privacy whether they will be guaranteed for their sensitive personal information they provides. It can be said that consumers will be willingly to trust less-known web vendors eventually, and after having a series of commercial transactions involving financial and sensitive personal information.

Some interviewees assumed that there can be hackers and also even if they do trust their familiar web vendors to protect their sensitive personal information, the web vendors might not pay attention to privacy of their sensitive personal information. The interviewee's thought can be revealed reflection of the connection between her concerns on privacy of her sensitive personal information and in turn, it leads to her perception on risks in order to transact with web vendors. A study of Privacy and Data Protection by Munir, in 2003, indicated that Malaysian consumers, in general, did not like if web vendors used their sensitive personal information for advertising without having their permissions, particularly, when sensitive personal information was distributed to other third parties for unintended purposes. The below citation demonstrates the interrelation between consumers' perceived privacy and perceived risk on e-commerce transactions.

> "Of course, there are always risks involved in dealing with e-commerce transactions. Those advertisements come after that, but I really do not like

to open junk e-mails. If I see this kind of e-mail, I immediately remove from my e-mail list without opening it. I don't think web vendors need to market their products by sending those advertisements frequently."

The interviewee mentioned that she does not like to open spam e-mails, and thus her view could be understood as an expression of the relationship between privacy and risk, since the spam e-mails generate risks in dealing with e-commerce transactions and trustworthiness of web vendors.

Some of the interviewees observed that web vendors ask many things that some are not necessary. And it is difficult to modify personal information, such as address provides to web vendor, and it possibly will be inconvenient, and they sense there may be risk involved in providing sensitive personal information to web vendors. Swaminathan et al. (2001) stated that frequent purchased online consumers were concerned on formation of new laws defending privacy in dealing with e-commerce transactions. Some consumers believe that web vendors do not have to ask much information about their consumers to effectively market products and services over the Internet. One of the interviewees said:

"When I wanted to buy flight tickets for my family through online service in here, they asked me to enter name, passport number, date of birth and passport expired date for all. It is impossible to give all on spot, so I had to cancel the transactions. I felt so uncomfortable and emailed to the Airline customer service that their service is not friendly user. Where as my friend from U.S.A told me that he only needs to provide his name to buy flight e-tickets to fly abroad."

For this type of consumers' viewpoints, it is easier for them if web vendors do not ask to give much sensitive personal information. Web vendors can provide adequate privacy policies in their online store sites, and their intensions on the collection and distribution of consumers' sensitive personal information in order to gain increased value from their consumers (Hann et al., 2007). The below quotation illustrates the most familiar approach to make sure consumers' privacy by avoiding possible risks when he or she is engaging with unfamiliar web vendors and also when he or she will not have sufficient trust on the particular web vendor.

> "Sometimes, I don't feel to enter all the information because I feel like it is just wasting of my time. But, when I have no choice, I enter incorrect date of birth, contact number and also, I have an e-mail account to provide when dealing with all kind of e-commerce transactions. I seldom check that e-mail account to delete all spam e-mails."

The interviewee noted a risk of being wasted time. Some interviewees were slightly worried about providing their sensitive personal information to web vendors. Therefore, consumers sometimes provide incorrect personal information in engaging commercial transactions over the Internet.

Sipior et al. (2004) indicated that consumers' privacy related to ethical issues over the Internet, namely, loss of anonymity, unintended uses of consumers' sensitive personal information, information sharing, direct marketing and so on were hindering consumers from dealing with e-commerce transactions. According to the authors, protecting consumers' privacy is both economic and ethical issue, and in order to promote the growth and development of e-commerce, it is essential to deal with the protection of consumers' concerns on privacy issues. Some of the interviewed consumers stated that ordering from the foreign web vendors across the border was not safe enough, or they would not feel comfortable for providing of their sensitive personal information to foreign online store sites. One of the interviewees was so concerned on privacy to deal with web vendors from different countries across the border because he noted that he had knowledge from media and also it would be difficult to make complaint to online store sites that had no bodily existence store in the same country or whose office might be only available aboard. The following quotation illustrates this issue.

> "What I understand is that we should not simply give our information to any web vendor or anywhere, especially to the foreign online stores. I think, if anything goes wrong on transaction, such as didn't receive ordered goods, it will not be easy to claim back and we may not know where to complain about that. In this case, our personal information will be used for unintended purposes."

The interviewee's thoughts exposed his interest in privacy exposures and the above citation showed the interrelation between interviewee's perceived privacy and perceived risk. The interviewee was slightly concerned on privacy as well as possible risks related to commercial transactions in dealing with unfamiliar foreign web vendors. However, another interviewee said:

> "I used to pay my credit card information to one of the Company for a certificate and also paid for some books and articles to foreign online stores. I know that my privacy might be threatened, but I have no choice because I needed that thing at that time. If it is essential for me and have no choice, I will have to give my personal information to online store sites abroad."

The interviewee revealed that although there can be privacy problems, he had to deal with the well-known or unfamiliar web vendors when it is necessary. Thus, sometimes, we have to engage in commercial transactions with unfamiliar web vendors when we have no choice and it is essential. It is not because we trust that web vendors to provide our sensitive personal information but because we have no choice.

Information privacy is the capability of the individuals to manage information about themselves over the web. As soon as individual cannot uphold the considerable level of control on their sensitive personal information and the handling of them, invasions of privacy arise. Consumers react in a different way to online privacy problems. It may be due to a cultural point of view. Different consumers usually have diverse judgments on what is unfair and what is fair in gathering and handling of their sensitive personal information in dealing with e-commerce transactions.

### 5.2.3 Trustworthiness of Web Vendors

Basically an element of trust is required for all kind of relationships. Since trust has continually been an essential issue to influence consumers' attitudes towards vendors, it already has been publicized to be of more important in web-based e-commerce environments. Given that trust plays a significant role in influencing consumer behaviour, building trust between web vendors and consumers is vital for the

continuous growth and development of e-commerce. Furthermore, trust together with commitment, communication and satisfaction is considered to be one of the essential elements affirming the offline marketing relationship, and thus the significance of trust in online marketing is regularly growing. The growth and development of e-commerce will not be able to reach its potential, without involving trust. Therefore, trust is the foundation upon which commerce is built and it is the means to the growth and development of electronic commerce transactions. (Eric, 2000; Florian, 2001; Grabner, 2002; Salam et al., 2003; Nam et al., 2006 and Hann et al., 2007).

Developing good relationships with online consumers pays off when all is going well but it can also pay big dividends when things go very wrong. Consumers' credit card data security and privacy breach cannot be a positive result between consumers and web vendors, but the way the web vendors handles it can mitigate the problem and make consumers feel like they are included in the solution, i.e. more like partners than like victims. Web vendors need to trust their consumers and their reaction to the news, and in turn, web vendors will be rewarded with a largely positive response from their consumers in social media.

Trust itself is not easy to observe and measure. Until now, the technical representations of trust have not really had anything to do with the average user, i.e. trust is not an issue to be handled with by the ordinary consumer, and all the security features are controlled by technical experts. However, with the rise of e-commerce and online transactions, it has become essential for non-technical individuals also to be able to handle their own security in a way and particularly to be able to manage, express and control their trust, such as who they trust online, in what situations and why, and to what extent. consumers will not automatically engage in e-commerce transactions, even though web vendors implements perfect systems for completely secure e-commerce transactions (Xiaowen and Gavriel, 2003), because secure technological infrastructure is only a basic foundation and by itself not adequate for building the level of trust needs for the growth and development of e-commerce transactions (Salam et al., 2003). An interviewee, who is a software engineer and technically advanced user, stated that:

"I am unfamiliar with seals of approval in dealing with e-commerce

transactions, and suspicious of them. For me, even though web vendors' reputation and brand name are important, there are differences in the amount of trust depending on what kind of service was dealt with. I do prefer to buy online but not only from well-known and familiar vendors. As long as no security warning signs appear, I'm willingly to buy from unknown vendors for a better price."

Therefore, the sources of online trust seem to vary, such as some trust the advice of a friend, some trust web vendors' reputation and brand name, some refer to media, magazine and newspaper for information and so on. Due to the fact that there is a similarity, in general, concerning the significance of trust for successful e-commerce, online organizations as well as those organizations which will adopt online business strategy shall not fail to realize the development of trust as a means and also as a process for the building of long-term relationship without emphasizing only on short-term and commercial transactional side of e-commerce.

In dealing with e-commerce, from the offline to online transfer of activities for business purposes involving financial and sensitive personal information forces web vendors to restructure the methods of traditional rules for developing reliability and trust can be employed. In stead of offering merely commercial transactional based scheme, online store sites should serve consumers' focus e-services effectively in order for the growth and development of e-commerce successfully.

A consumer attempting to take part in a business relationship with an online store sites involving financial and sensitive personal information has to begin with a positive trust. The increased on consumers' trust in e-commerce and the benefit e-commerce offers to consumers are two key factors to reduce consumers' concerns on privacy of their sensitive personal information. In addition, in order to gain for a certain degree of benefit from web vendors, consumers may be excited to reveal their sensitive personal information willingly to web vendors (Nam et al. 2006). However, one of the interviewees stated that:

"I found the product that I wanted with the cheap cost at Lelong store site. However, I do not have enough trust on the Lelong store to provide my

> credit card information and that's why, made decision to give more in my familiar store site. The offered price looked so good in Lelong, but I didn't have experience purchasing products from Lelong. I prefer to buy from well-known and familiar web vendors only."

When consumers are pleased with services offered by a particular online store site at the first time, the consumers will be likely to approach to that site to do more purchases. Therefore, trust can be easily built and is simply continued in the future if the consumer has pleasant experience with the online store site, at the first time. Consumers' trust in web vendors facilitates e-commerce transactions by reducing perceived risk (Pavlou and Gefen, 2004). The interviewee's thoughts revealed her interest in preferred online store site by noting:

> "Once I couldn't find one of my preferred store sites which provide great customer service and the site had all kinds of electronics brands. But I didn't have thought whether they are no more offering e-commerce services for their products. Actually, I had purchased product from that store before and I didn't mind to spend several minutes of trying to find that site again."

Most of the online-savvy consumers will prefer to pay more to web vendors who offer higher quality e-services. Trustworthiness of web vendors can be negatively affected by the online store site's quality, such as, the website has typing error, link is not working properly and so on (Xiaowen and Gavriel, 2003 and Florian, 2001). The interviewee's thoughts revealed that:

> "I do not care about price much if I will be treated with high quality e-services from online store. If I can not know my purchase details, i.e. if I can not view shipping information basically, I will not deal with that kind of store site mainly due to poor usability of that store site."

Thus, in order for web vendors to develop trustworthiness and reliability with their consumers, and remain consumers' protection, web vendors shall consider the focus on providing higher service quality in dealing with e-commerce transactions. When consumers conduct an online purchase from the foreign web vendors across the

border, they will have more concern as to whether they will receive high quality services. Therefore, for the global e-commerce environment, providing high quality e-services has become especially important.

Nowadays, online consumers have opportunity to compare the online store sites' service quality and choose a web vendor they feel comfortable to engage with involving financial and sensitive personal information. Providing high quality e-service is the key to success for any web vendor who is doing business in this competitive domestic and global e-commerce environment. Therefore, web vendors need to make great efforts to improve e-service of their online store sites.

In view of the fact that there are barriers to overcome, trust in business-to-consumer (B2C) is more difficult to establish compared to traditional commerce. The online store that exists over the web is often not real in the eyes of consumers. Consumers' lack of inherent trust in unfamiliar web vendors is coherent and to be expected. Therefore, if a web vendor wishes to do successful online business, proving trustworthiness is essential by satisfying consumers for several years as it grows.

Consumers draw on cues from the interface of online store site to decide the web vendor's purposes and their liabilities (Jens et al., 2003 and Batya et al., 2000). One of the interviewed consumers' thoughts revealed his perception on the competent and knowledgeable of the online store site by saying:

> "I do not feel comfortable making a purchase from a store site which do not provide the detailed information on all products. If the online store site mentioned almost no description of the product, I will never deal with that kind of store sites, mainly due to the lack of product information; though I knew detail information about that product from other sites. The web vendor may just ship me any old model if I deal with that kind of online store site."

Some of the interviewees placed more value on other features of online store sites, such as communities' forum, detailed information on products, contact details, and so on compared to online store sites' interface design. Interactive assessment supports, such as reference, the design helping consumers to search for existing products and to

assist in-depth comparisons amongst certain alternatives may have greatly attractive properties in terms of consumers' decision making (Hubl and Trifts, 2000). The interviewee noted that:

> "Even if I do not like online store site's layout, I don't care if I trust that site and I had experienced in dealing with that store site. I know that store site's design makes products nicer and better. I would prefer to conduct transaction with online store site which has poor design but provides communities' forums, detailed product information, detailed contact information."

The online store site is able to offer a very effective way to collect and bring out consumers' comments. The comments from experienced consumers can be a valuable asset to both the consumers and the online store sites. Besides, the oncoming online consumers do care about the price of the product, more significantly they need high quality service so that they will receive the product as ordered on time. Therefore, an individual online store site needs to understand consumer's purchase behaviour and to improve service quality and customer retention.

Consumers recognize that they can easily search for a good deal over the Internet, and thus, it is one of the main causes consumers deal with e-commerce transactions. Like traditional stores, online store sites also need to build strong relationship with their consumers in order to be successful in competitive online environment. With the use of emerging technology, online store sites basically have more potential and advantages than traditional stores.

### 5.2.4 Perceived Risk

When consumers disclose their sensitive personal information to web vendors throughout e-commerce transactions, they presume the risk of having their information threatened. Electronic commerce involves a diversity of risks, such as credit card information and product performance, that consumers concern (Salisbury et al., 2001) and their trust in web vendors facilitates e-commerce transactions by reducing perceived risk (Pavlou and Gefen, 2004). Since trust can reflect a readiness

to presume the risks of exposure, trust in e-commerce transactions may be observed as a function of consumers' risk. For that reason, when consumers concern the risk of security and privacy to be negligible, they could trust to adopt e-commerce transactions because risk in e-commerce transactions is mainly formed by information security and privacy threats.

When an individual engages in e-commerce transactions, he or she can not completely expect to trust that everything about his or her transaction is guaranteed as compared to dealing with offline store site. One of the interviewees who did not have experienced with online transactions said:

> "I have not ordered anything via online service. I do not feel comfortable to deal with online store sites because no physical interaction, cannot evaluate the product, cannot know whether the web vendor is legitimate. I want to pay only after receiving the goods or services. I want to see the real product first before buying it. I think, I cannot complain online store if I am not satisfy with the product. I do not want to receive junk e-mail and I also heard about viruses and increasing hacker attacks on media and newspapers."

It is obvious to say that dealing with e-commerce transactions, the consumer do not have physical contact with the web vendor, and as a result, is incapable to assess the products effectively and also to verify the identity of the unknown web vendor. In addition, since online payment is generally made before the delivery of the goods or services, the consumer's financial and sensitive personal information can be treated unfairly. The received product might not be the same with the product purchased. It will be difficult to make complaints to online store sites that have no bodily existence store or whose agency may not be available in the same country. In addition, the consumer noted the increasing problem with unwanted e-mail and increasing attack of online thieves in dealing with e-commerce transactions.

Trust can reduce consumers' perceived risk. Trust between a consumer and web vendor depends on trustworthiness, believing one another, and confidence in one another's opinion. When we do not trust each other, we neither engage in financial transactions nor allow ourselves to disclose sensitive personal information and

become more intimate. In reality, interactions between two people who do not trust one another are difficult to sustain, especially in online environment. The strong brand name and web vendor's reputation can influence consumers' perceived risk. The consumers' risk concerns related to e-commerce transactions may be influenced by several information sources, for example, recommendations, brand, and personalized information (Hong, 2002 and Deighton and Barwise, 2000). The interviewed consumer stated that:

> "I have only used Dell's e-service and bought laptop via their service. Other than that, I have not ordered anything through online environment. Because I do not want to take any risk in engaging with unknown store sites over the web."

In this situation, the well-known web vendor influenced the interviewee very much that the degree of her risk perceptions was reduced, which facilitated the interviewee to deal with a risky commercial relationship since she never had experienced with e-service before. In particular, the interviewee trusted the well-known brand and had enough confidence to engage in e-commerce transactions offered by well-known web vendor.

Some of the products are basically easier to purchase online compared to other products mainly due to involving extremely low risk. Thus, the matter of context in e-commerce transactions can influence consumers' perceived risk. The products, such as music, video, books, and magazines are cheaper and have extremely low risk factor, and transactions can be done very quickly and easiest way.

> "I prefer to purchase latest music and video online at online store sites that I had previous positive experiences with. These kinds of product are the cheapest and almost no risk involved."

It is true to say that the risks that the consumers have to face are really high in dealing with e-commerce transactions. In reality, online transactions are considered as being riskier procedures and building online trust to overcome consumers' perceived risk is not easy compared to the offline communication channels. However, there is more trust by reducing risk towards such online services with which trust has always been

an issue, even in the real world. The increase in institutional trust reduces consumers' perceived risk in e-commerce transactions (Salam et al., 2003). The interviewee stated that:

> "I pay for my bills through online banking services. I have not ordered anything from online store site. I heard that web marketers frequently send those advertisements to promote their products. I do not want to receive any spam e-mail. Also, I do not want to take any risk."

The above quotation illustrated the interviewee's trust in online banking services and she had not used any other e-services than bank's e-service. The citation also demonstrated the role of consumers' perceived risk related to e-commerce transactions, since the interviewee did say she did not have experienced in dealing with e-commerce rather than online banking service, because she was slightly concerned for possible risks to deal with e-commerce transactions. It can be said that trust towards a bank in the real world stays more or less the same when using the online banking services, and thus, trust in the real world is powerfully transferable to online environments in order to reduce consumers' perceived risk in dealing with online services.

Individuals' characteristics affect their view on the trustworthiness of web vendor where by leading to their risk concerns. Some individuals are suspicious by nature and thus, are full of uncertainties concerning how to look for available products and check out, whether their financial and sensitive personal information are safe and secure, and so on, in dealing with e-commerce transactions. Some individuals believe that the cheaper the product price, the smaller amount of risk they are dealing with, and thus, they try to reduce their risks by purchasing of the products and goods with the lowest prices over the web. On the other hand, when some consumers are determined by need, they give the impression to do whatever it took to make the purchases online.

Even though the Internet and World Wide Web together with the emerging information technologies have offered rapid growth of e-commerce transactions, e-commerce will not achieve its full prospective until consumers' perceived risks of dealing with e-commerce transactions have been decreased to a satisfactory level.

## 5.3 Chapter Summary

In summary, the findings from this study exposed numerous concerns regarding consumers' perceptions on security, privacy, trustworthiness of web vendors, and risk in dealing with e-commerce transactions. In accordance with our findings, four influential factors are in some way related collectively. The results from interviewees' perspectives supported that consumers' perceived security and perceived privacy were not mainly concerned to their trust in e-commerce transactions though consumers' perceived security and perceived privacy might slightly influence on the trustworthiness of web vendors in dealing with online store sites abroad. Furthermore, consumers' perceptions of the trustworthiness of the web vendors were also related to their perceived risks and the concern about privacy was also addressed to perceived risks.

The consumers may have enough trust in a particular web vendor; however, if any kind of privacy breaches occur, regarding their financial or sensitive personal information, trust may reduce and risk add to. These finding are, therefore, of interest to e-commerce marketers relative to perception on security, privacy, trust and risk of their consumers.

Next chapter will provide a discussion and conclusion based on the findings of this research. Both the limitations of the study and its implications will be discussed, and recommendations will be offered for further research.

# CHAPTER 6

# DISCUSSION AND CONCLUSION

## 6.1 Introduction

This research was undertaken to meet the primary objective to identify the factors that contribute to the consumers' willingness to engage in e-commerce transactions, and further study the relationship between those factors. Therefore, this study was focused on: (a) to study whether or not consumers' perceived security and privacy of online transaction significantly affect their confidence to adopt e-commerce, (b) to identify the factors of trust with web vendors to engage in transactions involving money and sensitive personal information, (c) to study the role of economic incentives and institutional trust related to consumers' perceived risk in order to adopt e-commerce, and (d) to study the relationship between security, privacy, trustworthiness of web vendors and risk perceptions in e-commerce adoption.

This chapter provides the theoretical as well as practical explanation of the empirical findings discussed in the analysis chapter together with the interviewees' perspectives, theoretical as well as practical implications and contribution to research, limitations of the study, recommendation for future research directions and conclusion.

## 6.2 Discussion of the Survey Research

The goal of this study was to identify influential factors which would aid consumers and web vendors in a mutually beneficial manner and potentially contribute to better utilization and growth of e-commerce. Distribution frequencies were established for the research variables, such as gender, age, race, education level, primary occupation,

Internet usage, online purchases, the reason for not buying online and opinion on online credit card security, and also for each of the study's research constructs, namely, perceived information security, perceived information privacy, trustworthiness of web vendors and perceived risk, economic incentives and institutional trust. The analysis of respondents' answers regarding information security and privacy concerns, trustworthiness of web vendors and risk concerns when dealt with questions about their trust on e-commerce transactions under seven hypothetical scenarios were examined through reliability analysis followed by factor analysis, pearson correlation coefficients and regression analysis.

### 6.2.1 Discussion of Demographic Data and Various E-Commerce Issues

#### 6.2.1.1 Study I

The paper-based survey population consisted of 89 full-time final year undergraduate students, who did not have experienced with online purchases, from two universities. Out of the questionnaires returned, 4 questionnaires were not usable because they were incomplete, such as more than 5 questions unanswered. The remaining participants comprised the sample (N=85) for the first study.

Regarding to non-online purchasers' study, the respondents were much balanced in terms of gender, 43 were male representing 50.6% of the overall respondents whereas 42 were female representing 49.4% of the overall respondents. In terms of age, the majority groups of the respondents (about 98.8%) were aged between 20 years old and 30 years old. The remaining (about 1.2%) were adults in their early 31's. In terms of race, the majority of the respondents from this survey were *Malay* race, representing 57.6% of the overall respondents followed by the *Chinese* race, representing about 18.8% of the total respondents. The remaining respondents consisted of Indian (about 15.3%) and other races (about 8.2%).

Even though most of the respondents were frequen user of the Internet, the respondents did not have experience in online purchases. Out of the 85 respondents, almost all the respondents (about 96.5%) reported that "they frequently use the Internet" while the remaining 3.5% reported that "they seldom use the Internet". Out

of 85 respondents who never purchased online before, about 49.4% were not willing to purchase in the near future, about 22.4% were willing to make online purchases but to a lesser amount and the remaining numbers of the respondents were willing to make more online purchases in the near future. The respondents who never purchased previously and also who were not willing to purchase online in the near future were asked about the reason for not buying online. The major reason (about 36.5%) was cited to be the concern on security and privacy of their personal data, about 8.2% were due to lack of time, about 27.1% were because of lack of interaction, about 22.4% were because of cannot feel the product, about 2.4% were because of the high prices, and the remaining about 3.5% were due to other reasons. All respondents were also asked about the opinion on credit card security for online purchases. The majority of the total respondents (about 54.1%) had the beliefs that "the use of credit card for online purchases is unsafe", while about 11.8% believed "somewhat safe". About 8.2% of the total respondents were indifferent for online credit card security and the remaining (24.7%) of the respondents were not sure about this.

#### 6.2.1.2 Study II

For the second study, the data utilized were collected using online survey instrument. The target group of respondents were the internet savvy general public. The survey link was posted on freesurveysonline.com and distributed to communities forums and blog of Malaysia's top e-commerce sites, namely, lelong.com.my, airasia.com and mphonline.com, for one month period (from 17 July 2009 to 17 August 2009). This online survey received 166 responses of which 163 met the stated measure. Therefore, total of these surveys (N = 248) were reviewed and analyzed.

As regards to online purchasers' study, one hundred and sixty three respondents (62.0% males and 38.0% females) were participated for the purpose of analysis for this study. The majority of the respondents (about 81.0%) were age between 20 to 30, followed by age between 31 to 40 (about 17.8%), while remaining about 1.2% were age between 41 to 50. The results showed that the sample was skewed towards age between 20 to 30, with the mean of 1.2 and standard deviation of 0.433. In term of

races, about 54.0% were Malay race, followed by Chinese race (about 23.3%), while about 12.9%% were Indian and about 9.8% were other races.

The majority of the respondents who participated in the survey were highly educated with most of the sample being degree holders. Out of the overall respondents, about 28.2% of the respondents had graduated at the diploma level, about 54.0% of the respondents were holding university degrees, and 17.2% of the respondents had master's degrees. The remaining numbers of the respondents (about 0.6%) were holding high school certificates. The respondents were having worked for different departments in a variety of positions such as administration, management, educator, sales personnel, and professional. The majority (about 46.0%) of the respondents were working in management level, followed by administrative assistants (about 21.5%). About 14.1% were working as sales personnel, educators (about 11.7%), and the remaining respondents were professional (about 6.7%). Out of the 163 online respondents, almost all the respondents (about 96.9%) reported that "they frequently use the internet" while the remaining 3.1% reported that "they sometimes use the Internet". The observation of the responses showed that respondents (about 50.3%) made online purchases "sometimes" followed by made online purchases "seldom" (about 49.1%), while only 0.6% made online purchases "always".

Out of the respondents who had purchased online previously, majority (about 52.1%) had made purchases between 1 year and 3 years, about 33.7% had made purchases between 4 years and 6 years, and about 14.1% had made purchases for less than 1 year. The respondents, who had made purchases on the Internet were also asked about the possibility of continued purchasing in the near future compared to previous purchases. Only 1.8% of the respondents were willing to reduce their future purchases compared to previous purchases, while majority (about 67.5%) were willing to maintain the same status by neither increasing nor decreasing their online purchases. About 30.7% were willing to make a bit more online purchases in the near future.

All the respondents were also asked about their opinions on credit card security for online purchases. The majority of the respondents (about 60.1%) believed that "the use of credit card for online purchases is somewhat safe" while about 22.1%

believed “somewhat unsafe”. About 15.3% of the respondents were indifferent on online credit card security and the remaining (about 2.5%) respondents believed “very safe”.

#### 6.2.1.3 Overall Study

Overall, two hundred and forty eight respondents (58.1% males and 41.9% females) were participated for the purpose of analysis for this study. The majority of the respondents (about 87.1%) were age between 20 to 30, followed by age between 31 to 40 (about 12.1%), while remaining about 0.8% were age between 41 to 50. The results showed that the sample was skewed towards age between 20 to 30, with the mean of 1.14 and standard deviation of 0.367. In term of races, about 55.2% were Malay race, followed by Chinese race (about 21.8%), while about 13.7% were Indian and about 9.3% were other races.

Out of the 248 overall respondents, almost all the respondents (about 93.1%) reported that “they frequently use the Internet” while about 5.6% reported that “they sometimes use the Internet”. The remaining 1.2% reported that “they seldom use the Internet”. All the respondents were also asked about their opinions on credit card security for online purchases. The majority of the respondents (about 43.5%) believed that “the use of credit card for online purchases is somewhat safe” while about 22.2% believed “somewhat unsafe”. About 12.9% of the respondents were indifferent on online credit card security while about 8.9% believed “very unsafe”. About 8.5% of the respondents were not sure about this while the remaining (about 2.0%) respondents believed “very safe”.

### 6.2.2 Discussion of Research Hypotheses

#### 6.2.2.1 Study I

The empirical findings of the first study showed the relative strength of trustworthiness of web vendors and perceived risk on consumers’ trust in e-commerce transactions as opposed to perceived information security and perceived information privacy. While information security and information privacy concerns had been

proposed as sufficient predictors towards building consumers' trust in e-commerce transactions, our results showed that the effects were insignificant, and thus not supporting for our proposed hypotheses (H1 and H2). This implies that perceived information security and perceived information privacy are not any more sufficient predictors of consumers trust in e-commerce adoption. This can be said that since consumers get familiar with the World Wide Web and with the emerging information technologies to safe and secure themselves in dealing with e-commerce transactions, their concerns on security issues are turning less significant matter from time to time. Moreover, it can be said that consumers may also get ready to follow defensive methods on themselves to care for their privacy in dealing with e-commerce transactions, such as giving untrue personal information to web vendors.

However, the influence of a consumer's perceived privacy of online transaction on trust was mediated by perceived security, supporting our proposed hypothesis (H3). This may be because the privacy concern of online consumers will be less sensitive matter if they believe that they are transacting over secure mediums. Our results also showed that trustworthiness of web vendor was a significant predictor of consumers' trust in e-commerce adoption, supporting our proposed hypothesis (H4). This can be said that consumers will prefer to transact with well-known vendors over the Internet.

Moreover, the construct of perceived privacy fairly manifested itself primarily through the trustworthiness of web vendors on consumers' trust in e-commerce transactions, supporting our proposed hypothesis (H5). This may be because the privacy concern of non-online purchasers will be less sensitive matter if they transact with well-known vendors over the Internet. In addition, the results showed that a high level of consumers' perceived risk would lower their trust in e-commerce transactions. We also found that the increased in economic incentives and the increase in institutional trust did not reduce a consumer's perceived risk in online transaction.

The regression analysis of this study showed that only two out of four predictors were found to be significant to the consumers' trust in e-commerce adoption. In overall, the regression model showed about 18% (Adjusted R Square = 0.178) of the consumers' trust in e-commerce adoption would be influenced by the consumers'

perceived security, perceived privacy, trustworthiness of web vendors, and consumers' perceived risk.

#### 6.2.2.2 Study II

A key empirical finding of second study showed the relative strength of perceived information privacy on consumers' trust in e-commerce transactions as opposed to perceived information security, trustworthiness of web vendors and perceived risk. Despite the fact that information security concerns had been proposed as influential predictor towards building consumers' trust in e-commerce adoption, our results showed that perceived information security did not have a statistically significant relationship with consumers' trust in e-commerce transactions. This implies that perceived information security is not any more a sufficient predictor of consumers' trust in e-commerce adoption. This can be said that since experienced online consumers get familiar with the World Wide Web and with the emerging information technologies to safe and secure themselves in dealing with e-commerce transactions, their concerns on security issues are turning less significant matter from time to time. However, perceived information privacy was still a sufficient predictor of consumers' trust in e-commerce adoption.

Moreover, the influence of a consumer's perceived privacy of online transaction on trust was mediated by perceived security, supporting our proposed hypothesis (H3). This may be because if consumers believe that they are transacting with secure mediums over the web, privacy concerns on their sensitive personal information will be less sensitive matter. The results showed that trustworthiness of web vendor and consumers' perceived risk did not have statistically significant relationships with consumers' trust in e-commerce adoption.

The construct of perceived privacy fairly manifested itself primarily through the trustworthiness of web vendors on consumers' trust in e-commerce transactions, supporting our proposed hypothesis (H5). This may be because the privacy concern of online consumers will be less sensitive matter if they transact with well-known vendors over the Internet. The results also showed that though the increase in institutional trust did not reduce a consumers' perceived risk in online transaction, the

increase in economic incentives reduced a consumers' perceived risk in online transaction, supporting our proposed hypothesis (H7). The regression analysis of the study showed that only one predictor out of four predictors was found to be slightly significant to the consumers' trust on e-commerce adoption.

#### 6.2.2.3 Overall Study

The hypotheses were developed to test the importance of perceived information security, perceived information privacy, trustworthiness of the web vendors, and perceived risk to explain the consumers' trust in e-commerce transactions. The empirical findings of the overall study showed the relative strength of perceived risk on consumers' trust in e-commerce transactions as opposed to perceived information security, perceived information privacy, and trustworthiness of web vendors.

While information security, information privacy, and trustworthiness of web vendors concerns have been proposed as sufficient predictors influencing consumers' trust in e-commerce transactions, our results showed that the effects were insignificant, and thus not supporting for our proposed hypotheses (H1, H2 and H4). This implies that perceived information security, perceived information privacy, and trustworthiness of web vendors are not any more sufficient predictors of consumers trust in e-commerce adoption. This can be said that since both non-online purchasers and online purchasers get familiar with the World Wide Web and with the emerging information technologies to safe and secure themselves in dealing with e-commerce transactions, their concerns on security issues are turning less significant matter from time to time. In addition, it can be said that non-online purchasers as well as online purchasers might also get ready to follow defensive methods on themselves to care for their privacy in dealing with e-commerce transactions, such as giving untrue personal information to web vendors. And also, in dealing with well-known web vendors and with the web vendors whom consumers had experienced and satisfied in engaging with financial and sensitive personal information, consumers may have enough confidence to trust in e-commerce transactions.

A strong influence of perceived information privacy on perceived information security and trustworthiness of the web vendors were identified. It can be said that if

consumers believe that they are transacting with secure mediums over the web with trusted web vendors, privacy concerns on their sensitive personal information will be less sensitive matter. The results also showed that institutional trust, such as banks and well-known credit card companies, influences consumers' perceived risk. This may be because consumers believe that there would be no financial risk involved since they are using banks and well-known credit card companies in dealing with web vendors, and also if anything goes wrong with transaction, they can later verify and claim. It was found that economic incentives, such as providing lower price and higher quality, do not influence consumers' perceived risk. However, economic incentives and institutional trust influence consumers' perceived information privacy. It can be said that consumers seem agreeable to being influenced by economic incentives and institutional trust for disclosure of their sensitive personal information.

The highest percentage appeared in perceived information privacy (91%), and the next highest percentages were shown in consumers' trust (65%) and trustworthiness of the web vendors (64%). Compared with the percentages of explained portions of those variables, those percentages of perceived information privacy (36%) and perceived risk (17 %) were lower.

### 6.3 Discussion of Interviewees' Perspectives

The findings from 15 interviewed consumers showed that some consumers were more confident to deal with web vendors from own country rather than foreign online stores by believing that web vendors from own country would handle security related issues more efficiently compared to foreign online stores. However, some consumers preferred to deal with online store sites abroad for better price. Therefore, even though web vendors carry out the scientific measurement of security with the use of emerging information technological solutions, it is consumers' perceptions of security that could power trust in dealing with e-commerce transactions.

Some consumers were slightly concerned about their privacy, that is, whether they would be guaranteed for their sensitive personal information they provided. Some of

the consumers observed that web vendors asked many things that some were not necessary. Therefore, different consumers usually have diverse judgments on what is unfair and what is fair in gathering and handling of their sensitive personal information in dealing with e-commerce transactions.

Most of the online consumers prefer to pay more to web vendors who offer higher quality e-services, communities' forum, detailed information on products and contact details compared to online store sites' interface design. Consumers recognize that they can easily search for a good deal over the Internet, and thus, it is one of the main causes consumers deal with e-commerce transactions. Like traditional stores, online store sites also need to build strong relationship with their consumers in order to be successful in competitive online environment. With the use of emerging technology, online store sites basically have more potential and advantages than traditional stores.

Some individuals were suspicious by nature and thus, were full of uncertainties to deal with e-commerce. Some individuals believed that the cheaper the product price, the smaller amount of risk they were dealing with, and thus, they tried to reduce their risks by purchasing of the products and goods with the lowest prices over the web. On the other hand, when some consumers were determined by need, they gave the impression to do whatever it took to make the purchases online. The findings also showed that the consumers might have enough trust in a particular web vendor; however, if any kind of privacy breaches occurred, regarding their financial or sensitive personal information, trust might reduce and risk added to.

## 6.4 Summary of the Research Findings

With the advancements in technology and the World Wide Web, e-commerce has become a major element in today's economy. The growth and development of e-commerce is an important element in the growth of the country economy by contributing a positive factor for society. However, a thorough review of the literature revealed that consumers' concerns on security, privacy, trustworthiness of web vendors and risk had presented a serious limitation to the development and growth of

e-commerce. Additionally, the literature review revealed that managing consumers' security, privacy, trustworthiness of web vendors and risk concerns might be a means to boost the growth and development of e-commerce. However, with the increasing numbers of consumers engaging in e-commerce transactions nowadays as a daily life, their perceptions on previously influential factors might not be significant barriers for the growth and development of e-commerce. To contribute toward this gap was the focus of this research.

The purpose of this study was to study the influential factors of consumers' willingness to trust in e-commerce transactions in order to establish a consensus among Malaysian consumers to adopt e-commerce and develop a framework that could be generalized to consumers from developing countries. This study focused on answering the following three main questions particularly.

a) Do consumers' security and privacy concerns of online transaction significantly relate to their trust in e-commerce adoption?
b) How do the trustworthiness of the web vendors relate to the consumers' adoption of e-commerce?
c) How do economic incentives and institutional trust relate to consumers' perceived risk in order to adopt e-commerce?
d) What are the inter-relationships of security and privacy concerns, trust beliefs and risk perception, and how do these factors affect consumers' behaviour intention to adopt e-commerce?

The answers to these questions were considered to help web vendors, perhaps, to find the means to relieve consumers' concern on security, privacy, trust and risk related to e-commerce transactions. The mitigation of consumers' concerns on these issues would be one way to enhance the growth and development of e-commerce and, corresponding to the growth of the country economy. The economy growth and development are benefiting society by bringing constructive changes to the lives of many individuals and to the country. This study was carried out by asking the target population of Internet savvy students and general public, what their intentions and opinions were about trusting e-commerce transactions, which were associated with security, privacy, trust and risk issues.

The intentions and opinions agreed by the respondents were best suited for a quantitative survey study. The paper-based survey questionnaires were distributed to undergraduate students, who did not have experienced with online purchases, from two universities. Furthermore, due to the important role played by the Internet in this study involving e-commerce, the best way to reach to the Internet savvy general public was considered to be through an e-survey. Therefore, the research was undertaken through the paper-based and electronic surveys. Data from the 248 respondents were analyzed using the SPSS and AMOS statistical software. Upon analysis of the data, it was concluded that perceived information security and perceived information privacy did not have statistically significant relationships or associations with non-online purchasers' trust to adopt e-commerce. However, trustworthiness of web vendors and perceived risk have statistically significant relationships or associations with non-online purchasers' trust in e-commerce transactions. On the other hand, perceived information security, trustworthiness of web vendors and perceived risk do not have significant relationships with online purchasers' trust in e-commerce transactions while perceived information privacy has somewhat significant relationship with online purchasers' trust in e-commerce transactions.

In order to know more about consumers' views on their perceptions regarding the study constructs, a semi-structured theme interview was included with the fact that it was valuable in a condition where a wealthy amount of information was required to create opportunities to realize the occurrence as largely as possible and to produce new insights. The findings showed that consumers' perceived security and perceived privacy were related to the construct of perceived risk and therefore, ultimately to the construct of trustworthiness of web vendor. Furthermore, consumers' perceptions of the trustworthiness of the web vendors were also related to their perceived risks and the concern about privacy was also addressed to perceived risks. The findings also indicated that consumers' perceived privacy might directly influence on trustworthiness of web vendors in dealing with online store sites abroad.

## 6.5 Addressing the Research Objectives

One of the biggest challenges that web vendors have faced and continued to deal with is the understanding of their consumers. While a lot has been known about how consumers think and act in the traditional commerce world, there has still not been enough effort put into understanding the consumers to willingly trust in e-commerce transactions. The consumer has the double identity of both a traditional consumer and a computer user. Simultaneously, the emergence of the online store site that also bears a double identity of a traditional store where information technology has come to the foreground and has actually become the online store itself. Therefore, it is required to realize how the consumers think and act in dealing with online store sites.

The main objective of this study is to identify the factors that contribute to the consumers' willingness to engage in e-commerce transactions, and further study the relationship between those factors.

The findings of the studies can be summarized as follows:

### 6.5.1 Perceived Information Security

We have found that perceived information security could have no significant impact on consumers' trust in e-commerce transactions. When we tested the impact of perceived security on consumers' trust in e-commerce transactions, our results showed no differences in each of the three empirical studies. These findings were in contrast with many researches on security and privacy concerns in dealing with e-commerce (Pavlou and Chellappa, 2001; Belanger et al., 2002; Ahuja et al., 2003; Kai et al., 2004; Laforet and Li, 2005; and Ahmed et al., 2007). This can be said that since consumers get familiar with the World Wide Web and with the emerging information technologies to safe and secure themselves in dealing with e-commerce transactions, their concerns on security issues are turning less significant matter from time to time.

Nevertheless, our findings from one of the interviewees' perspectives indicated that perceived security might directly influence on trust in dealing with online store sites abroad. Therefore, it is crucial for web vendors abroad to enhance consumers' security concerns in order to lead to more online purchases that turn to an increase in

overall sales. Even if web vendors guarantee the security of consumers' sensitive personal information by the use of latest secure information technologies, it is consumers' perception of security that will power trust.

### 6.5.2 Perceived Information Privacy

When we tested the impact of perceived information privacy on consumers' willingness to trust in e-commerce transactions, our results varied in the three empirical studies. In the first study, perceived information privacy was insignificant for consumers' trust in e-commerce transactions. It can be said that consumers may prepare to adopt protective measures on themselves to protect their own privacy online, such as providing incorrect personal information when dealing with web vendors. These findings contradicted with the study of Malhotra et al. (2004), in which the researchers stated that privacy concern was seen as a major threat to e-commerce. The overall study's findings also showed no significant association between perceived privacy and consumers' trust in e-commerce transactions.

In the second study, however, we have found that perceived information privacy can have slight significant impact on consumers' trust in e-commerce transactions. In addition, some interviewees assumed that there could be hackers and also the web vendors might not care about their sensitive personal information. However, they do trust their familiar web vendors to secure their privacy in dealing with e-commerce transactions. As suggested by Hann et al. (2007), web vendors could provide adequate privacy policies in their online store sites, and their intensions on the collection and distribution of consumers' sensitive personal information in order to gain increased value from their consumers.

Therefore, it is essential to understand the consumers' concerns generally related to their privacy, their proficiency in the Internet and emerging information technologies, and the way they analyze the role of web vendors as well as the role of the governmental regulations in defending their privacy. Moreover, consumers habitually have diverse opinions on what is unfair and what is fair in gathering and handling of their sensitive personal information by web vendors in dealing with e-commerce transactions.

### 6.5.3 Trustworthiness of Web Vendors

The findings varied in the three empirical studies when we tested the impact of trustworthiness of web vendors on consumers' willingness to trust in e-commerce transactions. In the first study, our results showed that trustworthiness of web vendor had a significant relationship with the consumers' trust in e-commerce transactions. This could be said that consumers would prefer to transact with well-known vendors over the Internet. These results agreed with many researchers (Eric, 2000; Florian, 2001; Grabner, 2002; Salam et al., 2003; Nam et al., 2006; and Hann et al., 2007) who stated that trust wa the foundation upon which commerce was built and it was the key to the growth and success of electronic commerce transactions.

However, the results of the second study showed that trustworthiness of web vendors did not have a statistically significant relationship with consumers' willingness to trust in e-commerce transactions. The findings from overall study also showed no significant relationship between trustworthiness of web vendors and consumers' trust in dealing with e-commerce transactions. This could be said that in dealing with well-known web vendors and with the web vendors whom consumers had experienced and satisfied in engaging with financial and sensitive personal information, consumers might have enough confidence to trust in dealing with e-commerce transactions.

The findings from interviewees' perspectives revealed that the sources of trust related to e-commerce transactions might be varied, such as some trusted the advice of a friend, some trust web vendors' reputation and brand name, some referred to media, magazine and newspaper for information and so on. Since there is confirmation of a common similarity concerning the importance of trust for successful e-commerce, online organizations as well as those organizations which will adopt online business strategy should not fail to realize the development of trust as a means and as a process for continuous relationship building without emphasizing only on temporary and commercial transactional area of e-commerce.

### 6.5.4 Perceived Risk

When we tested the impact of perceived risk on consumers' trust in e-commerce transactions, our results varied in the three empirical studies. The empirical findings of the first study and overall study showed the relative power of perceived risk on consumers' trust in e-commerce transactions. This might be because when an individual engages in e-commerce transactions, the consumer could not completely expect to trust that everything about his or her transaction was guaranteed as compared to dealing with offline store site. These results agreed with Jarvenpaa et al. (2000), in which the authors found that the risk perception associated with online transaction might reduce the consumer's perception of control and as a result, might influence the consumers' willingness to trust in online transactions. However, the results of the second study showed that perceived risk did not have a statistically significant association with consumers' trust in e-commerce transactions.

Consumers' trust in web vendors facilitated e-commerce transactions by reducing perceived risk (Pavlou and Gefen, 2004). The Interviewed consumers perceived risk in different ways. Individuals' personalities affect their view on trustworthiness of web vendor where by leading to their risk concerns. Some individuals are suspicious by nature and thus, are full of uncertainties regarding how to check out, if their financial and sensitive personal information are safe, if the shipping price and dates are feasible and so on, in dealing with e-commerce transactions. Some individuals believe that the less the product costs, the less risk they are taking, and thus, they try to reduce their risk by shopping for the products and goods with the cheapest prices over the web. On the other hand, when some consumers were determined by need, they gave the impression to do whatever it took to make the purchases online.

Therefore, e-commerce will not achieve its full prospective until consumers' perceived risks of dealing with e-commerce transactions have been decreased to a satisfactory level, even though the Internet and World Wide Web together with the emerging technologies have offered rapid growth of e-commerce transactions.

## 6.6 Implications and Contribution to Research

The consumers' trust in electronic commerce transactions might be promising. The web vendors have to look for ways to justify the consumers' concerns with the intention that e-commerce can develop and, sequentially, develop the country economy as a whole. Web vendors have to understand that, in general, consumers are unwilling to provide their sensitive personal information to engage in e-commerce transactions. According to our empirical findings, the trustworthiness of web vendors and perceived risk were identified as the influential factors for non-online purchasers' trust in e-commerce transactions while perceived information privacy was identified as the influential factor for online purchasers' trust in e-commerce transactions. With the purpose of gaining non-online purchasers' awareness and openness, web vendors have to, most likely, concentrate on establishing trust with them. However, the growth and development of e-commerce should not be focused only on trustworthiness of web vendors, perceived risk, and perceived information privacy as the influential factors to achieve consumers' trust in e-commerce transactions.

Moreover, our findings from interviewees' perspectives revealed several issues concerning their perceptions on security, privacy, trustworthiness of web vendors, and risk in dealing with e-commerce transactions. The findings showed that all four concepts were in some way linked together, i.e. consumers' perceived security and perceived privacy were related to the construct of perceived risk and therefore, ultimately to the construct of trustworthiness of web vendor. Furthermore, consumers' perceptions of the trustworthiness of the web vendors were also related to their perceived risks and the concern about privacy was also addressed to perceived risks. The findings also indicated that consumers' perceived privacy might directly influence on trustworthiness of web vendors in dealing with online store sites abroad.

Since it appears that some of the interviewees' perceived security and perceived privacy have a direct influence on their perceived risk, perceived security and perceived privacy may ultimately affect on consumers' trust in e-commerce transactions. Therefore, the consumers might have enough trust in a particular web vendor; however, if any kind of security and privacy breach occurs related to the consumer's financial or sensitive personal information, trust may reduce and risk add

to. These finding are, therefore, of interest to e-commerce marketers relative to perception on security, privacy, trustworthiness of web vendors and risk of their consumers.

The developing and validating of an integrative framework for the adoption of e-commerce at the individual level are the key contributions of this study. In the research model, consumers' perceived security, perceived privacy, trustworthiness of web vendors and perceived risk are included as associating factors for e-commerce adoption.

This study provides the implications for both theoretical development and practical implementation. This study provided a major contribution for theory development by incorporating concerns for security, privacy, trustworthiness of web vendors and risk in the theoretical framework of TRA. Consumers' concerns persuade their impressions which eventually determine on the intention and behaviour. It is essential to include the factors of consumers' perceived security, perceived privacy, trustworthiness of web vendors and perceived risk for the framework of e-commerce because a consumer needs to make decision to take part in e-commerce in a community of trustworthiness and risk perception, which sequentially is affected by security and privacy concerns. For privacy literature, this study adds by highlighting the role of trustworthiness of web vendors as an effect of consumers' perceived privacy.

The use of the Internet, the economy and e-commerce become significant elements of any individual's life. If consumer wants to deal more with online services offered by web vendors, they have to demand and request for what they really wish for, for example, adequate control on their financial and sensitive personal information, nationwide legislations and so on. Alternatively, web vendors have to carefully realize their consumers' demands. Consumers' needs and requirements may differ based on different age group, gender, education, race and individual's other features. Web vendors have to make effort to encounter every consumer's requirements for the reason that the growth and development of e-commerce will contribute to the enlargement of the economy, and in turn, all of the humanity will be benefited eventually.

## 6.7 Limitations of the Study

This study has several limitations that affect the reliability and validity of the findings. The study did not take into account gender biases, cultural biases, income and other demographic characteristics with the research hypotheses. Further, the sample size participated in the study might have affected the findings of this study and it might also limit the generalisability of the findings. With the sampling procedure, there were chances that the responses provided might not be the true reflection of the population in general and the findings might not represent Malaysian consumers as a whole; therefore, any generalisation of the findings may not be 100% reliable.

This study focused on the perception of consumers on perceived security and privacy, the trustworthiness of web vendors and perceived risk to trust in e-commerce transactions rather than looking into the consequences of perceived security and perceived privacy, the trustworthiness of web vendors and perceived risk on consumers' actual purchasing behaviour. According to Dinev and Hart (2006), even though the measuring of perception was normally assumed as a measuring of actual behaviour, assessing the consumers' actual behaviour could make the validation of the study stronger.

The model might have excluded other possible influential factors for the consumers' trust in e-commerce transactions (i.e., the study did not consider other beliefs, such as perceived usefulness, perceived ease of use, Internet experience, and so on).

Future studies can also link other demographic variables of consumers as well as web vendors' reputation, site's usefulness and ease of use. These dimensions may provide interesting recommendations on the difference in the consumers' trust building mechanisms to be adopted in dealing with e-commerce.

## 6.8 Recommendations for Further Study

The current studies were only managed to scratch the surface of what determined the consumers' attitudes towards e-commerce transactions. Much further study is needed until we have a clear picture of the major factors that influence the way consumers feel, think, make decisions, and purchase on the online store sites. The study focused particularly on consumers' perceptions on security, privacy, trustworthiness of web vendors, and risk in dealing with e-commerce transactions. This study could be considered as the stepping stone for other studies in order to give complete realization of consumers' concerns related to information security and privacy, trustworthiness of web vendors, and risk in dealing with e-commerce transactions. This study focused on the respondents' perceived behaviour instead of their actual behaviour.

In this study, the respondents were asked their perceptions on general e-commerce adoption. Further study can improve this study by asking the subjects to provide responses with regard to a specific e-commerce, such as m-commerce.

We have seen that economic incentives can influence the consumers' perceived privacy in dealing with e-commerce transactions. Future study can focus on consumers' actual behaviour for disclosing their sensitive personal information in trade for monetary and economic incentives in dealing with e-commerce transactions. Further research might also determine the certain degrees of consumers' control over their sensitive personal information provided to web vendors in dealing with e-commerce transactions.

Future study on this topic can concentrate on the gender basis among consumers in dealing with e-commerce relative to their perceptions on security and privacy, trustworthiness of web vendors and risk. For example, a study should focus on whether male consumers are more eagerly to reveal their financial and sensitive personal information by more trusting of e-commerce compared to female consumers in trade for monetary and economic incentives in dealing with e-commerce transactions.

Future study can concentrate also on the consumers' different age groups in dealing with e-commerce relative to their perceptions on security and privacy,

trustworthiness of web vendors and risk. The reason behind the willingness to trust in e-commerce transactions of different age groups might be the theme of future study.

Future studies should also concentrate on the consumers' different culture backgrounds and its impacts on readiness to trust in e-commerce transactions. Since the Internet and e-commerce are not limited with geographical borders, consumers from different culture backgrounds might provide different perceptions on security and privacy, trustworthiness of web vendors and risk in dealing with e-commerce transactions.

## 6.9 Conclusion

This study concludes that while trustworthiness of web vendors is a critical factor in explaining non-online purchasers' trust in e-commerce transactions, it is important to pay attention to their risk concern on e-commerce transactions. Though in previous researches, security and privacy appeared to be the top main concerns for consumers' trust in e-commerce adoption, the empirical findings of this study indicated that there were poor associations between consumers' perceived security and consumers' trust, and between consumers' perceived privacy and consumers' trust. This may be because consumers get used to the Internet and to the techniques that can be used to protect themselves online, the security and privacy are becoming less sensitive matters over as time. As trustworthiness of web vendors lies at the heart of enduring Business-to-Consumer e-commerce relationship, web-based organizations need to find ways of improving consumers' concerns on trustworthiness in order to utilize fully the prospective of e-commerce.

The consumers' concerns for security and privacy were used to be the major barriers that needed to be considered before they reached the level to adopt e-commerce. The findings from this study also indicated that perceived privacy was still to be the slight concern for online purchasers' trust in e-commerce adoption, though there was a poor correlation between perceived security and online consumers' trust. Clear privacy policies should be posted on the commercial websites, and

shortcomings on privacy of sensitive personal information may result in serious consequences. Web based organizations should place adequate control to ensure privacy of consumers' sensitive personal information by implementing effective mechanism to address any violation.

Overall, e-commerce will not achieve its fullest prospective until consumers' perceived risks of dealing with e-commerce transactions have been decreased to a satisfactory level, even though the Internet and World Wide Web together with the emerging technologies have offered rapid growth of e-commerce transactions. First of all, web-based organisations will have to realize and, subsequently, make effort to satisfy their consumers by providing their consumers' demands for the growth and development of their online businesses.

REFERENCES


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.

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

Ahuja, Vijay. (1997). 'Secure Commerce on the Internet'. *Boston: AP Professional*

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

Ajzen, I. (1991). 'The Theory of Planned Behavior." *Organizational Behavior and Human Decision Processes*, 50(2), 179-211.

Alan L.H. (2000). 'Finally, Someone knows what he's talking about.' *Hydraulics & Pneumatics,* Vol. 54, No.12, p.4.

Aldas-Manzano, J., Lassala-Navarre, C., Ruiz-Mafe, C., Sanz-Blas, S. (2009), "The role of consumer innovativeness and perceived risk in online banking usage", *International Journal of Bank Marketing*, Vol. 27 No.1, pp.53-75.

Anandarajan, M., Simmers, C. and Igbaria, M. (2000). An exploratory investigation of the antecedents and impact of the Internet usage: an individual perspective. *Behavior and Information Technology*. Vol. 19, pp. 69-85.

Andrea Basso, David Goldberg, Steven Greenspan, and David Weimer (October 2001). First impressions: Emotional and cognitive factors underlying judgments of trust ecommerce. In *EC'01*, 137 - 143, Tampa, Florida, USA.

Anil Gurung (May 2006). Empirical Investigation of the Relationship of Privacy, Security and Trust with Behavioral Intention to Transact in E-Commerce. *ProQuest Information and Learning Company*.

Anita Lifen Zhao, Nicole Koenig-Lewis, Stuart Hanmer-Lloyd, and Philippa Ward, (2010). Adoption of internet banking services in China: is it all about trust?, *International Journal of Bank Marketing,* Vol. 28, No. 1, pp. 7-26.

Applegate, L. M.; Austin, R. D. and McFarlan, F.W. (2002) 'Creating Business Advantage in the Information Age'. *McGraw-Hill Higher Education.*

Arbuckle James L. (2007). AMOS 18 Users Guide. *Amos Development Corporation.*

Ashrafi, N., & Kuilboer, J. (2005). Online privacy policies: An empirical perspective on self-regulatory practices. *Journal of ElectronicCommerce in Organizations*, Vol. 3, No. 4, pp. 61-74.

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.

Babita Gupta, Lakshmi S. Iyer, and Robert S. Weisskirch (2010). Facilitating Global E-Commerce: A Comparison of Consumers' Willingness to Disclose Personal Information Online in the U.S. and in India, *Journal of Electronic Commerce Research*, Vol. 11, No. 1, pp. 41-52.

Bagozzi, R. P., and Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, Vol. 16, pp. 74-94.

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

Batya Friedman, Jr. Peter H. Kahn, and Daniel C. Howe (December 2000). Trust online. *Communications of the ACM*, Vol. 43, No. 12, pp. 34 - 40.

Belanger, F., Hiller, J. S., and Smith, W. J. (2002), "Trustworthiness in Electronic Commerce: The role of Privacy, Security, and Site attributes", *The Journal of Strategic Information Systems*, Vol. 11, No. 3-3, pp. 245-270.

Belanger France, and Carter Lemuria (2008). Trust and risk in e-government adoption, *Journal of Strategic Information Systems*, Vol. 17, pp: 165–176.

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.

Bond, R. (2002) 'The New Economy Excellence Series - New Economy Equity-Navigating Security and Legal Issues in Digital Business'. *John Wiley & Sons, Ltd.*

Braithwaite, T. (2002) 'Securing E-Business Systems- a Guide for Managers and Executives'. *New York: John Wiley & Sons, Inc*.

Brancheau, J. and Nansi, S. (2001) 'Essential Technologies for E-Commerce'. *Prentice Hall*

Brannen, L., (2007). Privacy matters. *Business Finance,* Vol. 13, No. 7, pp. 20-22.

Brown, R., and Riley-Katz, A. (2008). E-commerce holding steady with incentives. *WWD: Women's Wear Daily*, Vol. 196, No. 127, 14-1NULL.

Bush, A., Bush, V., and Harris, S. (1998). 'Advertiser perceptions of the Internet as a marketing communications tool.' *Journal of Advertising Research*, Vol. 38, No. 2, pp. 17-27.

Carlos Flavián, and Miguel Guinalíu, (2006). 'Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site.' *Industrial Management & Data Systems*, Vol. 106, No. 5, pp.601-620.

Carroll, J. and Broadhead, R. (2001). 'Selling Online- How to Become a Successful E-Commerce Merchant.' *Canada: Dearborn Trade, a Kaplan Professional Company.*

Cary, C., Wen, H., and Mahatanankoon, P. (2003). 'Data mining: Consumer privacy, ethical policy, and systems development practices.' *Human Systems Management*, Vol. 22, No. 4, pp. 157-168.

Caudill, E., and Murphy, P. (2000). Consumer online privacy: Legal and ethical issues. *Journal of Public Policy & Marketing*, Vol. 19, No. 1, pp. 7-19.

CCRC Staff (2005, April 11) 'Fraud in the Internet'. [Online]. Available: http://www.crime- research.org/articles/Internet_fraud_0405/2

Cha, Young-Seock. (2002, Oct 16). *E-Commerce Security Technologies*. [Online]. Available:

http://secinf.net/firewalls_and_VPN/Ecommerce_Security_Technologies_Fire _ Wall.html

Chang, M. K., Cheung, W., and Lai, V. S. (2005), "Literature derived reference models for the adoption of online shopping", *Information & Management*, Vol. 42, No. 4, pp. 543-559.

Chellappa, R. K. (2003) 'Consumers' Trust in Electronic Commerce Transactions: The Role of Perceived Privacy and Perceived Security'. *University of Southern California, LA*. [Online]. Available: http://asura.usc.edu/~ram/rcf-papers/sec-priv.pdf.

Chellappa, R. K., and Sin, R. G. (2005) 'Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma'. *Information Technology and Management,* Vol. 6, pp. 181–202.

Cheswick, William R. and Bellovin, Steven M. (1994) 'Firewalls and Internet Security: Repelling the Wily Hacker'. *MA: Addison-Wesley.*

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.

Chou, David C. (2001) 'Integrating TQM Into E-Commerce'. *Information System Management*. Vol.18, No. 4, pp. 31-39.

Churchill, Gilbert A. Jr. (1988) 'Basic Marketing Research'. *The Dryden Press*.

Clay Posey, Paul Benjamin Lowry, Tom L Roberts and T Selwyn Ellis (2010). Proposing the online community self-disclosure model: the case of working professionals in France and the U.K. who use online communities, *European Journal of Information Systems,* Vol. 19, pp. 181–195.

Coakes, S. J. and Steed L. G. (1999) 'SPSS: Analysis Without Anguish'. *Jacaranda Wiley Ltd.*

Consumer Reports poll (2008, September 25 ). Americans extremely concerned about Internet privacy. *U.S. Newswire*.

Consumer Web Watch Research Report (April 16 2002). A matter of trust: What users want from web sites. Princeton Survey Research Associates, [Online]. Available: http://www.consumerwebwatch.org.

Creswell, J., (2007). Qualitative inquiry & research design: Choosing among five approaches. *Thousand Oaks*, CA: Sage.

Cunningham, M. (2000) 'Smart Things To Know About E-Commerce'. *Capstone Publishing Limited.*

Culnan, M. (2000). "Protecting privacy online: Is self-regulation working?" *Journal of Public Policy & Marketing*, Vol. 19, No. 1, pp. 20-26.

Culnan, M., and Armstrong, P. (1999). "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation." *Organization Science*, Vol. 10, No. 1, pp. 104-115.

Culnan, M. J., and Bies, R. J. (1999). "Managing Privacy Concerns Strategically: The Implications of Fair Information Practices for Marketing in the Twenty-first Century." Visions of Privacy: Policy Choices for the Digital Age, C. J. Bennett and R. Grant, eds., University of Toronto Press, Toronto, ON, pp. 149-167.

Cynthia L. Corritore, Susan Wiedenbeck, and Beverly Kracher (2001). The elements of online trust. In *CHI 2001*, pp. 504 - 505.

Das, S., Echambadi, R., McCardle, M., and Luckett, M. (2003). 'The effect of interpersonal trust, need for cognition, and social loneliness on shopping, information seeking and surfing on the Web.' *Marketing Letters*, Vol. 14, No. 3, pp. 185-202.

Dauda, Y., Santhapparaj, AS., Asirvatham, D. and Raman, M. (Aug 2007), "The Impact of E-Commerce Security, and National Environment on Consumer adoption of Internet Banking in Malaysia and Singapore," *Journal of Internet Banking and Commerce*, Vol. 12, No. 2, pp. 1-10.

David Gefen (2002). Reflections on the dimensions of trust and trustworthiness among online consumers. In the *DATA BASE for Advances in Information Systems*, Vo. 33, No. 3, pp. 38-53.

Deepak Sirdeshmukh, Jagdip Singh, and Barry Sabol (January 2002). Consumer trust, value, and loyalty in relational exchanges. *Journal of Marketing*, Vol. 66, pp. 15-37.

Dekker M. (1997) 'Security of the Internet'. *The Froehlich/Kent Encyclopedia of Telecommunications*, Vol. 15, pp. 231-255.

De Vaus, D. (2002). Survey in social research (5th edn.). St Leonards: Routledge.

Deighton, J., and Barwise, P. (2000). 'Digital marketing communication', *Future Media Working Paper*, No. 00-801, London Business School, UK.

Dhillon, G., and Moores, T. (2001). Internet privacy: Interpreting key issues. *Information Resources Management Journal*, Vol. 14, No. 4, p. 33.

Dhillon, G., Bardacino, J., and Hackney, R. (2002) "Value Focused Assessment of Individual Privacy Concerns for Internet Commerce." *Proceedings of the Twenty Third International Conference on Information Systems*, Barcelona, Spain.

Dholakia, R. P., Zhao, M., Dholakia, N., & Fortin, D. R. (2000). Interactivity and revisits to Websites: A theoretical framework. *RITIM working paper*, [Online]. Available: http://ritim.cba.uri.edu/wp/

Dierks, T. and Allen C. (1999). The Transport Layer Security Protocol. *Internet RFC 2246*.

Diffie, Whitfield 'Security Technologies'. *Sun Microsystems.*

Dinev, T., and Hart, P. (2006). Privacy concerns and levels of information exchange: An empirical investigation of intended e-services use. *Eservice Journal*, Vol. 4, No.3, pp. 25-59.

Diwan, P. and Singh, D. (2001) 'Computer Networks & E-Commerce'. *Golden Books.*

Dommeyer, C. J., and Gross, B. L. (2003). "What Consumers Know and What They Do: An Investigation of Consumer Knowledge, Awareness, and Use of Privacy Protection Strategies." *Journal of Interactive Marketing*, Vol. 17, No. 2, pp. 34-51.

Doney, P.M., Barry, J.M., Abratt, R. (2007), "Trust determinants and outcomes in global B2B services", *European Journal of Marketing*, Vol. 41 No.9/10, pp.1096-116.

Dong-Her, S.; Chiang Hsiu-Sen, Chan Chun-Yuan, Binshan Lin, (2004). 'Internet security: malicious e-mails detection and protection', *Industrial Management and Data Systems*, Vol. 104, No. 7, pp.613 – 623.

Doraswamy, N. and Harkins, D. (1999) 'IPSes: The New Security Standard for the Internet, Intranets, and Virtual Private Networks'. *Upper Saddle River*, NJ: Prentice Hall PTR

Ecommerce-Guide (2002, July 2) 'E-Commerce Alert: Consumer Protection'. [Online]. Available: http://www.e-commercealert.com/article504.html.

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

Egger, F. N. (2001) 'Affective Design of E-Commerce User Interfaces: How to Maximise Perceived Trustworthiness'. Proceedings of the International Conference on Affective Human Factors Design. *Asean Academic Press*, London.

Electronic Payments: From Online Bill Payment to Credit Cards — Statistics, Strategies and Trends, (June 2003) [Online]. Available: http://www.emarketer.com

Elena Delgado-Ballester and Miguel Hernández-Espallardo (2008). Effect of Brand Associations on Consumer Reactions to Unknown On-Line Brands, *International Journal of Electronic Commerce*, Vol. 12, No. 3, pp. 81-113.

Elisabeth Davenport (April 2000). Non-contractual trust, design, and human and computer interactions. In *CHI 2000*.

Eric M. Uslaner (December 2000). Social capital and the net. *Communications of the ACM*, Vol. 43, No. 12, pp. 60 - 64.

Essinger, J. (2001) 'Internet Trust and Security'. *Addison-Wesley.*

Faja, S., Silvana, & Trimi, S. (2006). Influence of the Web vendor's interventions on privacy-related behaviors in e-commerce. *Communications of AIS*, Vol. 17, pp. 593-634.

FBI National Press Office. (2004, November 18) 'ID Theft/Credit Card Protections'. [Online]. Available: http://www.crime-research.org/news/18.11.2004/802/.

Feigenbaum, J., Parkes, D., & Pennock, D. (2009). Computational challenges in e-commerce. *Communications of the ACM*, Vol. 52, No.1, 70-74.

Felton, B. (2005, December 24) 'Cyber security breaches threaten, 2006 forecasts'**.** [Online]. Available: http://www.crime-research.org/analytics/1718/2.

Fleenor, J. (1999). SPSS 9.0 for Windows. *Personnel Psychology*, *52*(3), 833-835.

Florian N. Egger (2001). Affective design of e-commerce user interfaces: How to maximise perceived trustworthiness. In *Proceedings of the International Conference on Affective Human Factors Design*, London, Asean Academic Press.

Fogg B.J., Jonathan Marshall, Othman Laraki, Alex Osipovich, Chris Varma, Nicholas Fang, Jyoti Paul, Akshay Rangenekar, John Shon, Preeti Swani, and Marissa Treiman (2001). What makes web sites credible? A report on a large quantitative study. In *CHI 2001 Conference on Human Factors in Computing Systems*, pp. 61 - 68. ACM Press.

Ford, W. (1994) 'Computer Communications Security: Principles, Standard Protocols and Techniques'. *Upper Saddle River*, NJ: Prentice Hall PTR

Ford, W. and Baum, M.S. (2001) Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption, 2nd edition, *Upper Saddle River*, NJ: Prentice Hall.

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.

Furnell, S. M.; Karweni, T. (1999). 'Security implications of electronic commerce: a survey of consumers and businesses', *Internet Research*, Vol. 9, No. 5, pp.372–382.

Garcia, M. M. (2004). "Institutions and the Adoption of Electronic Commerce in Mexico, *Electronic Commerce Research Journal*, Vol. 4, No. 3, pp.201-219.

Garfinkel, S. and Spafford, G. (2001) 'Web Security, Privacy & Commerce.' *O'Reilly & Associates, Inc.*

Gefen, D., Karahanna, E., and Straub, D. W. (2003). 'Trust and TAM in Online Shopping: An Integrated Model.' *MIS Quarterly*, Vol. 27, No. 1, pp. 51-90.

Gefen, D., Straub, D. W., and Boudreau, M.-C. (2000). 'Structural Equation Modeling and Regression: Guidelines for Research Practice.' *Communications of AIS*, Vol. 4, No. 7, pp. 1-78.

Gervey, B., and Lin, J. (2000). 'Obstacles on the Internet.' *Advertising Age*, Vol. 71, pp. 12-22.

Ghosh, A.K. (1998) 'E-commerce Security: Weak Links, Best Defenses'. New York: *John Wiley & Sons, Inc*.

Ghosh, A. K. (2001) 'E-commerce Security and Privacy'. *Kulwer Academic Publishers.*

Ghosh, J. (2001, October 23) 'Ideal security in e-commerce'. [Online]. Available: http://www.ciol.com/content/flavour/entpr_sec/101102301.asp.

Godwin, J. U. (2001) "Privacy and security concerns as major barriers for e-commerce: a survey study", Information Management & Computer Security, Vol. 9, No. 4, pp. 165-174.

Golubev, V. (2004, March 9) 'Internet fraud: volumes are increasing'. *Computer Crime Research Center*. [Online]. Available: http://www.crime-research.org/news.

Goralski, W. and Waclawski, D. (1999) 'Virtual Private Networks: Achieving Secure Internet Commerce and Enterprisewide Communications'. *Computer Technology Research Corp.*, Charleston, South Carolina, USA.

Grabner-Kraeuter S. (2002) The role of consumers' trust in online-shopping. *Journal of Business Ethics*, Vol. 39, pp. 43-50.

Grace B. J., and Bollen A. K. (2005) Interpreting the Results from Multiple Regression and Strucctural Equation Models. *Bulletin of the Ecological Society of America*, pp. 283-295.

Graeff, T., and Harmon, S. (2002) Collecting and using personal data: Consumers' awareness and concerns. *Journal of Consumer Marketing*, Vol. 19, No. 4/5, pp. 302-318.

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.

Green, S. B. and Salkind, N. J. (2003) Using SPSS for Windows and Macintosh: Analyzing and understanding data (3rd edn.). *Upper Saddle River*: Prentic Hall.

Green River Community College 'Research Methods in the Social Sciences'. [Online]. Available: http://www.instruction.greenriver.edu/bahl/E112/methods.htm

Grupe, F., Kuechler, W., & Sweeney, S. (2002). Dealing with data privacy protection: An issue for the 21st century. *Information Systems Management*, Vol. 19, No. 4, p. 61-70.

Gurau, C.; Ranchhod, A. and Hackney, R. (2003) 'Customer-Centric Strategic Planning: Integrating CRM in Online Business Systems'. *Information Technology and Management*. Vol. 4, pp. 199-214.

Hackney, R.; Burn, J. and Dhillon, G. S. (2003) 'Strategic Planning for E-Commerce Systems (SPECS): Value Returns and Customer Alliance'. *Information Technology and Management.* Vol. 4, pp. 135-138.

Hair, J. F., Tatham, R. L., Anderson, R. E., & Black, W. (1998) 'Multivariate Data Analysis', 5th ed., *Upper Saddle River*, NJ: Prentice Hall.

Hair, J. F.; JR.; Bush, R. P. and Ortinau, D. J. (2000) 'Marketing Research : A practical approach for the new millennium'. *McGraw-Hill.*

Hair, J. F., Samouel, P., Babin, B., and Money, A. H. (2005) 'Essentials of Business Research Methods', *John Wiley & Sons Inc*.

Hann, I., Hui, K., Lee, S., and Png, I. (2007). Overcoming online information privacy concerns: An information-processing-theory approach. *Journal of Management Information Systems*, Vol. 24, No. 2, pp. 13-42.

Harrison-Walker, L. J. (2001). E-complaining: A content analysis of an Internet complaint forums. *Journal of Service Marketing*, Vol. 15, No. 5, pp. 397-412.

Hassler, V. (2001) 'Security Fundamentals for E-Commerce'. Norwood: *Artech House*

Hawkins, S., Yen, D.C. and Chou, D.C. (2001), 'Awareness and challenges of internet security', *Information Management & Computer Security*, Vol. 8, No. 3, pp. 131-143.

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

Heckathorn, D. (2007). Extensions of respondent-driven sampling: Analyzing continuous variables and controlling for differential recruitment. *Sociological Methodology,* Vol. 37, pp. 151-208.

Hedelin, L. and Allwood, C. (2002). 'IT and strategic decision making, *Industrial Management and Data Systems*', Vol. 102, No. 3/4, pp. 125-139.

Heijden, H. and Van D. (2001) 'Measuring IT Core Capabilities for Electronic Commerce'. *Journal of Information Technology*. Vol. 16, pp. 13-22.

Heshan Sun (2010). Transferring Attributes of E-Commerce Systems into Business Benefits: A Relationship Quality Perspective, *Journal of Electronic Commerce Research*, Vol. 11, No. 2, pp. 92-109.

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

Hoffman, D., Novak, T., and Peralta, M. (1999a). "Building Consumer Trust Online." *Communications of the ACM*, Vol. 42, No. 4, pp. 80-85.

Hoffman, D. L., Novak, T. P., and Peralta, M. A. (1999b). "Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web." *Information Society*, Vol. 15, No. 2, pp. 129-139.

Hong-Youl Ha (October 2002). The Effects of Consumer Risk Perception on Pre-purchase Information in Online Auctions: Brand, Word-of-Mouth, and Customized Information, *Journal of Computer-Mediated Communication*, Vol. 8, No. 1, pp.1-10.

Horton, R. P., Tamsin Buck, Patrick E. Waterson and Chris W. Clegg. (2001). Explaining intranet use with the technology acceptance model. *Journal of Information Technology*, Vol. 16, No. 5, pp. 237-249.

Hubl, G., and Trifts, V. (2000). Consumer decision making in online shopping environments: The effects of interactive decision aids. *Marketing Science*, Vol. 19, No. 1, pp. 4-21.

Hwang, W., Jung, H., and Salvendy, G. (2006). Internationalisation of ecommerce: A comparison of online shopping preferences among Korean, Turkish and U.S. populations. *Behaviour & Information Technology*, Vol. 25, No.1, pp. 3-18.

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, No. 1/2, pp.23–35.

Ida Madieha Azmi, (2002) 'E-commerce and privacy issues: An analysis of the personal data protection bill'. *Internal Review of Law Computers and Technology*, Vol. 16, No. 3, pp. 317-330.

IDC Malaysia, (24 January, 2007) "IDC Reports 70% Growth in Malaysia eCommerce Spending in 2006," [Online]. Available:

http://www.idc.com.my/PressFiles/IDC%20Malaysia%20-%20eCommerce.asp.

Iglesias, V., de Belen, I. A., & Vazquez, R. (2001). The effects of brand associations on the consumer response. *Journal of Consumer marketing*, Vol. 18, No.5, pp. 410-425.

Jakob Nielsen (January 1999). User interface directions for the web. *Communications of the ACM*, Vol. 42, No. 1, pp. 65 – 72.

Jarvenpaa, S.J., & Todd, P.A. (1997). Consumer reactions to electronic shopping on the World Wide Web. *International Journal of Electronic Commerce*, Vol. 1, No. 2, pp. 59-88.

Jarvenpaa, S. L., Tractinsky, N., Saarinen, L., and Vitale, M. (1999). "Consumer Trust in an internet store: a cross-cultural validation." *Journal of Computer-Mediated Communication*, Vol. 5, No. 2, pp. 1-10.

Jarvenpaa, S. L., Tractinsky, N., and Vitale, M. (2000). "Consumer trust in an internet store." *Information Technology and Management*, Vol. 1, No. 1-2, pp. 45-71.

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: Analysing the Statutes in Malaysia.* The Journal of American Academy of Business, Cambridge. Vol. 4, No. 1/2, pp. 55-63.

Jens Riegelsberger, M. Angela Sasse, and John D. McCarthy (April 5 - 10 2003). Shiny happy people building trust? photos on e-commerce websites and consumer trust. In *CHI 2003*, 5, Ft. Lauderdale, FL, USA.

Judith S. Olson and Gary M. Olson (December 2000). i2i trust in ecommerce. *Communications of the ACM*, Vol. 43, No.12, pp. 41– 44.

Justine Cassell and Timothy Bickmore (December 2000). External manifestations of trustworthiness in the interface. *Communications of the ACM*, Vol. 43, No.12, pp. 50-56.

Kai "O" Orni, Saana Kaleva, Soile Hirvashniemi, and Terttu Kortelainen. (2004) Usability of websites contributing to trust in e-commerce in *Trust in*

*Knowledge Management and Systems in Organizations*, 125 - 146. Idea Group Publishing, Hershey, PA, USA.

Kalakota, R. and Whinston, A. B. (1997) 'Electronic Commerce – A Manager's Guide'. *Addison Wesley Longman, Inc*.

Kaner, C. (1997, September) 'The Insecurity of the Digital Signature'. [Online]. Available: http://www.badsoftware.com/digsig.htm.

Katherine J. Stewart. (December 1999) Transference as a means of building trust in world wide web sites. In *Proceedings of the Twentieth International Conference on Information Systems*, Charlotte, NC, USA, pp. 459 – 464.

Katherine J. Stewart and Ross A. Malaga (2009). Contrast and Assimilation Effects on Consumers' Trust in Internet Companies, *International Journal of Electronic Commerce*, Vol. 13, No. 3, pp. 71-94.

Kessler, G.C. and Pritsky, N. T. (2000) 'Internet Payment Systems: Status and Update on SSL/TLS, SET, and IOTP', *Information Security Magazine*, pp. 1-20.

Kelly, E. P. and Erickson, G. S. (2005). 'RFID tags: commercial applications v. privacy Rights', *Industrial Management and Data Systems*, Vol. 105, No. 6, pp. 703-713.

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

Khosrowpour, Mehdi. (2004) 'IT Solutions Series: E-Commerce Security: Advice from Experts'. *CyberTech Publishing.*

Kimery, K. M., and McCord, M. (2002). 'Third-party Assurances: Mapping the Road to Trust in E-retailing.' *Journal of Information Technology Theory and Application*, Vol. 4, No. 2, pp. 63-81.

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.

Kolsaker, A. and Payne, C. (2002) 'Engendering trust in e-commerce: a study of gender-based concerns'. *Marketing intelligence & Planning*. Vol. 20, No. 4, pp. 206-214.

Krishnamurthy, S. (2001). A Comprehensive analysis of permission marketing. *Journal of Computer-Mediated Communication*, Vol. 6, No. 2. [Online]. Available: http://www.ascusc.org/jcmc/vol6/issue2/krishnamurthy.html.

Krishnamurthy, S. (2003) 'E-Commerce Management'. *Thomson South- Western Publication.*

Krishnan, G., (2006) "Internet marketing exposure in Malaysia," [Online]. Available: http://www.gobalakrishnan.com/2006/12/malaysia-internet-marketing/.

Kwek Choon Ling, Lau Teck Chai, and Tan Hoi Piew (July 2010). The Effects of Shopping Orientations, Online Trust and Prior Online Purchase Experience toward Customers' Online Purchase Intention, International Business Research, *Published by Canadian Center of Science and Education,* Vol. 3, No. 3, pp:63-76

Kyu Kim and Bipin Prabhakar. (December 2000). Initial trust, perceived risk, and the adoption of internet banking. In *Proceedings of the 21st International Conference on Information Systems*, pp. 537-543, Brisbane, Queensland, Australia.

Labuschagne, L. and Eloff, J.H.P. (2000) 'Electronic commerce: the information security challenge'. *Information Management & Computer Security*. Vol. 8, No. 33, pp. 154-157.

Laforet, S. and Li, X., (2005) "Consumers' attitudes towards online and mobile banking in China", *International Journal of Bank Marketing*, Vol. 23, No. 5, pp. 362-380.

Landau, S. and Everitt, B. S. (2004) 'A Handbook of Statistical Analyses using SPSS'. *Chapman & Hall/CRC.*

Lanier, C. D. Jr., and Saini, A. (2008). 'Understanding consumer privacy: A review and future directions.' *Academy of Marketing Science Review, 1.*

Laudon, K. C. and Traver, C. G. (2002) 'E-commerce: business, technology, society'. *Addison Wesley.*

Lee, M. (2001 July-September) 'The Adoption and Diffusion of Electronic Commerce'. *Journal of Global Information Management*. Vol. 9, No.3, pp. 1-10.

Lee, M.K.O., Turban, E., (2001). A trust model for consumer Internet shopping. *International Journal of Electronic Commerce,* Vol. 6, No. 1, pp. 75–91.

Leebaert, D. (1998) 'The Future of the Electronic Marketplace'. *Cambridge Mass.*

Leedy, P. D., and Ormrod, J. E. (2005). Practical research planning and design. *Upper Saddle River*, NJ: Pearson Prentice Hall.

Lepkowska, E. (2003) 'Internet Shopping: Perceptions of Offline and Online Consumers'**.** [Online]. Available: http://www.hicbusiness.org/BIZ2003Proceedings/ Elzbieta%20Lepkowska-White.pdf.

Liao, Z. and Cheung, M.T. (2003) 'Challenges to internet e-banking'. *Communications of the ACM*, Vol. 46, No. 12, pp. 248-250.

Liebermann, Y. and Stashevsky, S. (2002) 'Perceived risks as barriers to Internet and e-commerce usage'. *Qualitative Market Research: An International Journal*, Vol. 5, No. 4, pp. 291-300.

Littler, D., Melanthiou, D. (2006), "Consumer perceptions of risk and uncertainty and the implications for behaviour towards innovative retail services: the case of internet banking", *Journal of Retailing and Consumer Services*, Vol. 13 No.6, pp. 431-43.

Liu, C., Marchewka, J., and Yu, C., (2004) "Beyound Concern: A Privacy-Trust-behavioral intention model of electronic commerce", *Information & Management*, Vol. 42, No. 1, pp. 127-142.

Loney, M. (2003, July 7) 'E-commerce special report: Security'. *ZDNet UK*. [Online]. Available: http://insight.zdnet.co.uk/internet/ecommerce/0,39020454,2137147,00.htm.

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.

Loscocco, P. A.; Smalley, S. D.; Muckelbauer, P. A.; Taylor, R. C., Turner, S. J. and Farrell, J. F. (2003) 'The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments'. *National Security Agency.*

Luo X., (2002) "Trust Production and Privacy Concerns on the Internet, A Framework Based on Relationship Marketing and Social Exchange Theory", Industrial Marketing Management, Vol. 31, pp. 111-118.

Lynch, P., and Beck, J. (2001, 4th Quarter). 'Profiles of Internet buyers in 20 countries: Evidence for region-specific strategies.' *Journal of International Business Studies*, Vol. 32, No. 4, p. 725.

Malaysia's E-Commerce Statistics, (2009), [Online]. Available: http://malaysiacrunch.blogspot.com/2009/09/malaysias-e-commerce-statistics.html.

Malhotra, N. K. (2002) 'Basic Marketing Research- applications to contemporary issues'. *Prentice Hall.*

Malhotra, N. K., Kim, S. S., and Agarwal, J., (2004) "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and A Causal Model", Information Systems Research, Vol. 15, No. 4, pp. 336-355.

Marcella, A. J.; Jr., S., L. and Sampias, W. J. (1998) 'Electronic Commerce; Control Issues for Securing Virtual Enterprises'. *The institute of Internal Auditors.*

Markowski, R. (2004) 'Computer Architectures for E-Commerce'. [Online]. Available: http://www.webwisdom.com/edu_content/cis710_2spr04/lectures/module8/M8_II_2004_6.pdf.

Martins, A., Martins, N. and Olivier, M. S., (2001). 'Consumer Perception of Electronic-Commerce'. *South African Computer Journal.* Vol. 27, pp. 27-33.

McKenna, A. (2001). Playing fair with consumer privacy in the global online environment. *Information & Communications Technology Law*, Vol. 10, No. 3, pp. 339-354.

McKnight, D., Cummings, L. L., and Chervany, N. L. (1998). "Initial Trust Formation in New Organizational Relationships." *Academy of Management Review*, Vol. 23, No. 3, pp. 473-490.

McKnight, D. H., Choudhury, V., and Kacmar, C. (2002a). "Developing and validating trust measures for e-commerce: An integrative typology." *Information Systems Research*, Vol. 13, No. 3, pp. 334-359.

McKnight, D. H., Choudhury, V., and Kacmar, C. (2002b). "The impact of initial consumer trust on intentions to transact with a web site: a trust building model." *The Journal of Strategic Information Systems*, Vol. 11, No. 3-4, pp. 297-323.

McLaren, C. H. and McLaren, B. J. (2000) 'E-commerce Business on the Internet'. *South-Western Educational Publishing*.

Metzger, M. J. (2004, July) 'Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce'. *Journal of Computer-Mediated Communication*, Vol. 9, No. 4. [Online]. Available: http://jcmc.indiana.edu/vol9/issue4/metzger.html.

Michael Breward, (2007). Perceived Privacy and Perceived Security and Their Effects on Trust, Risk, and User Intentions, Eighth World Congress on the Management of eBusiness (WCMeB 2007), IEEE.

Microsoft. (2004, March 1) 'Shop Online More Safely' [Online]. Available: http://www.microsoft.com/windows/ie/using/articles/shopping.mspx

Miers, Derek. (2003) 'The Strategic Challenges of Electronic Commerce'. Retrieved January 28, 2004. [Online]. Available: http://www.enix.co.uk/electron.htm

Milberg, S., Smith, H., & Burke, S. (2000). Information privacy: Corporate management and national regulation. *Organization Science*, Vol. 11, No. 1, pp. 35-57.

Miller, Sandra Kay. (2001, April 5) 'Hardened OSes boost e-commerce security'. InfoWorld Test Center. [Online]. Available: http://archive.infoworld.com/articles

Milne, George R. (2000). 'Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue', *Journal of Public Policy and Marketing*, Vol. 19, (spring), pp. 1-6.

Milne, G., and Rohm, A. (2000). 'Consumer privacy and name removal across direct marketing channels: Exploring opt-in and opt-out alternatives.' *Journal of Public Policy & Marketing*, Vol. 19, Vol. 2, pp. 238-249.

Miniwatts Marketing Group (September 30, 2009) 'Internet Usage and World Population Statistics'. [Online]. Available: www.internetworldstats.com.

Mitchell, V. W. (1999). Consumer perceived risk: Conceptualizations and models. *European Journal of Marketing*, Vol. 33, No. 1/2, pp. 163-195.

Miyazaki, A. (2008). Online privacy and the disclosure of cookie use: Effects on consumer trust and anticipated patronage. *Journal of Public Policy & Marketing*, Vol. 27, No. 1, pp. 19-33.

Miyazaki, A. and Fernandez, A. (2000). Internet privacy and security: An examination of online retailer disclosures. *Journal of Public Policy & Marketing*, Vol. 19, No. 1, pp. 54-61.

Miyazaki, A. and Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer Affairs*, Vol. 35, No. 1, pp. 27-37.

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.

Moores, T.T. and Dhillon, G. (2003) 'Do privacy seals in e-commerce really work?'. *Communications of the ACM*, Vol. 46, No. 12, pp. 265-271.

Mozilo, A. (2001). 'Ensuring consumer privacy through high, flexible standards.' *Mortgage Banking*, Vol. *61, No.* 7, p. 15.

Munir, A.B. (2003) 'E-Commerce and the Law on Privacy'. Singapore: *Thomson*.

Mustafa Zakaria and Mohd Khairuddin Hashim, (October 2003) "Malaysian SMEs perceptions of e-business: some empirical evidence," *Paper presented at National Seminar on Electronic Commerce, Sunway Lagoon Resort Hote, Seangor*.

Muther, A. (2002) 'Customer Relationship Management: Electronic Customer care in the new economy'. Berlin; NY: *Springer.*

Nadia Santiago (September 24, 2009). Interview types: Structured, semi-structured, and unstructured. [Online]. Available: http://www.examiner.com/x-19273-San-Jose-Scholarly-Research-Examiner~y2009m9d24-Interview-types-Structured-semistructured-and-unstructured

Nam, C., Song, C., Lee, E., and Park, C. (2006). Consumers' privacy concerns and willingness to provide marketing-related personal information online. *Advances in Consumer Research*, Vol. 33, No. 1, pp. 212-217.

Naveen Amblee and Tung Bui (2008). Can Brand Reputation Improve the Odds of Being Reviewed On-Line? *International Journal of Electronic Commerce*, Vol. 12, No. 3, pp. 11-28.

Nedungadi, P., Chattopadhyay, A., and Muthukrishnan, A. V. (2000). 'Category structure, brand recall and choice', *Working Paper*, INSEAD, 2000/81/MKT, France.

Norhayati Abd Mukti, (2000) “Barriers to putting businesses on the Internet,” *The Electronic Journal on Information Systems in Developing Countries*, Vol. 2, No. 6, pp. 1-6.

Nugent, J. H. and Raisinghani, M. S. (2002). “The Information Technology and Telecommunications Security Imperative: Important Issues and Drivers”, *Electronic Commerce Research Journal*, Vol. 3, No. 1, pp.1-14.

O’daniel, T. (2000) ‘Electronic commerce’. *Pelanduk Publications.*

Olivero, N., and Lunt, P. (2004). ‘Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control.’ *Journal of Economic Psychology*, Vol. 25, No. 2, pp. 243-262.

Olkowski, David J., Jr. (2001). ‘Information Security Issues in E-Commerce.’ *SANS Institute*.

Oz, Effy. (2002) ‘Foundations of E-Commerce’. *Upper Saddle River*, NJ: *Prentice Hall* PTR, Natalie E. Anderson Publisher.

Paola Benassi (1999). TRUSTe: an online privacy seal program. *Communications of the ACM*, Vol. 42, No. 2, pp. 56–59.

Parissa Pourhosseini (2009). The Relationship of Financial Incentives and Consumers' Willingness to Disclose Information to e-Commerce Marketers. *ProQuest Information and Learning Company.*

Patricia Lanford, (July, 2004) What Is the Process By Which People Make a Purchase on the Internet?: A Qualitative Case Study. *Technical Report*. Auburn University. [Online]. Available: ftp://ftp.eng.auburn.edu/pub/techreports/csse/04/CSSE04-07.pdf.

Pavlou, P.A. and R.K. Chellappa ( January 2001), "The Role of Perceived Privacy and Perceived Security in the Development of Trust in Electronic Commerce Transaction", *Ebizlab Working paper*, p. 39.

Pavlou, P. A., (2003). “Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model”, International Journal of Electronic Commerce, Vol. 7, No. 3, pp. 69-103.

Pavlou, P. A., and Gefen, D. (2004). "Building effective online marketplaces with institution-based trust." *Information Systems Research*, Vol. 15, No. 1, pp. 37-59.

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.

Perry, J. T. and Schneider, G. P. (2001). 'New Perspectives on E-commerce'. *Thomson Learning.*

Pfleeger, C. (1997) 'Security in Computing'. (2nd ed.). *Upper Saddle River*, NJ: Prentice Hall PTR.

Phelps, J., D'Souza, G., and Nowak, G. (2001). 'Antecedents and consequences of consumer privacy concerns: An empirical investigation.' *Journal of Interactive Marketing*, Vol. 15, No. 4, pp. 2-17.

Phelps, J., Nowak, G., and Ferrell, E. (2000). "Privacy concerns and consumer willingness to provide personal information." *Journal of Public Policy & Marketing*, Vol. 19, No. 1, pp. 27-41.

Poindexter, J., Earp, J., & Baumer, D. (2006). An experimental economics approach toward quantifying online privacy choices. *Information Systems Frontiers, Vol.* 8, No. 5, pp. 363-373.

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

Qusay, Mahmoud (2000, March 1) 'Securing Component-Based E-Commerce Applications'. Retrieved April 23, 2006. [Online]. Available: http://advisor.com/Articles.nsf/aid/MAHMQ03

Rappa, Michael. 'Security & Encryption'. [Online]. Available: http://digitalenterprise.org/security/security.html

Rashidah Minakhatun (February 2007). E-Commerce Adoption in Malaysia: Factors Influencing Consumers' Confidence. *Unpublished Thesis*, International Islamic University Malaysia.

Ratnasingam, P. and Phan, D. D. (2003) 'Trading Partner Trust in B2B e-commerce: A Case Study'. *Information Systems Management*, Summer, pp. 39-50

Regan, Keith. (2003, May 8) 'Is Internet Security Killing E-Business'? [Online]. Available: http://www.crmbuyer.com/perl/story/21462.html.

Regan, P., (2003) "Privacy and Commercial Use of Personal Data: Policy developments in the United States, *Journal of Contingencies and Crisis Management*, Vol. 11, No. 1, pp. 12-18.

Roberts, Paul. (2003) 'FBI Warns of Spike in Identify Thefts'. [Online]. Available: http://www.pcworld.com/news/article.

Rohit Khare and Adam Rifkin (1998). Trust management on the world wide web. *Computer Networks and ISDN Systems*, Vol. 30, pp. 651-653.

Romano, N. C., Jr. (2003) 'Electronic Commerce Customer Relationship Management: A Research Agenda'. *Information Technology and Management*. Vol. 4, pp. 233-258.

Romm, Celia T. and Sudweeks, Fay. (1998). 'Doing Business electronically: A Global Perspective of Electronic Commerce.' *NY: Springer.*

Roznowski, J. (2003). A content analysis of mass media stories surrounding the consumer privacy issue: 1990-2001. *Journal of Interactive Marketing*, Vol. 17, No. 2, pp. 52-69.

Rush, Laura. (2004) 'E-Commerce Growth Will Impact SMBs'. [Online]. Available: http://ecommerce.internet.com/news/news/article.

Russell Hardin. (2001). Trust in Society, chapter Conceptions and Explanations of Trust. *Russell Sage Foundation*, New York.

S. Lelieveldt Consultancy. (2001, December 12) 'Research study on the integration of e-payments into the online transaction process'. *Institute for Prospective Techno-logical Studies*. [Online]. Available: http://epso.jrc.es/project/IntegrationwholeTPfinalreportres.pdf.

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.

Salisbury, W., David, R. A., Pearson, A., Pearson, W., & Miller, D. W. (2001). Perceived security and World Wide Web purchase intention. *Industrial Management & Data Systems*, Vol. 101, No. 4, pp. 165-176.

Sallehudin, Mohd Lip (2001) 'E-Commerce, E-Trading and Internet Money Transaction'. *11th Malaysian Law Conference*, Kuala Lumpur, Malaysia, [Online]. Available: http://www.mlj.com.my/free/articles.

Sara Jones, Marc Wilikens, Philip Morris, and Marcelo Masera (December 2000). Trust requirements in e-business: A conceptual framework for understanding the needs and concerns of different stakeholders. *Communications of the ACM*, Vol. 43, No. 12, pp. 81 -87.

Saunders, C. (2004). "Consumers Confidence Increasing in E-Commerce, Despite Threats." [Online]. Available: http://www.ecommerce-guide.com/news/trends/article.php/3440101.

Schwartz, S. (2001). SPSS 10. *Macworld*, Vol. 18, No. 3, p. 98.

Sergios Dimitriadis, and Nikolaos Kyrezis (August 2010). Linking trust to use intention for technology-enabled bank channels: The role of trusting intentions, *Psychology and Marketing,* Vol. 27, No. 8, pp. 799-820.

Shankar, V., Smith, A.K. and Rangaswamy, A. (2000). 'Customer Satisfaction and Loyalty on Online and Offline Environments', *Smith School of Business*, University of Maryland, College Park, MD.

Shanks, Tansley, & Weber (2003). Using ontology to validate conceptual models. *Communications of the ACM*, Vol. 46, No. 10, pp. 85-89.

Shareef, Mahmud Akhter , Kumar, Uma, and Kumar, Vinod (2008). Role Of Different Electronic-Commerce (EC) Quality Factors On Purchase Decision: A Developing Country Perspective, Journal of Electronic Commerce Research, Vol. 9, No. 2, pp. 92-113.

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

Sheehan, K., & Hoy, M. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing*, Vol. 19, No. 1, pp. 62-73.

Singh, T., and Hill, M. E. (2003) "Consumer Privacy and the Internet in Europe: a View from Germany." *Journal of Consumer Marketing*, Vol. 20, No. 7, pp. 634-651.

Sipior, J. C., Ward, B. T. and Rongione, N. M. (2004) 'Ethics of Collecting And Using Consumer Internet Data'. *Information System Management*, Vol. 21 No. 1, pp. 58-66.

Sirat, Abdullahi (2003) 'Exploring Factors Affecting Consumer Adoption of E-Commerce'. *Unpublished Thesis*, International Islamic University Malaysia.

Sithamparam, S. (2001) 'E-Commerce, E-Trading and Internet Money Transactions'. *11th Malaysian Law Conference*, Kuala Lumpur, Malaysia

Smith, G. E. (2004) 'Control and Security of E-Commerce'. *John Wiley & Sons.*

Smith, M. L. and Glass, G. V. (1987) 'Research and evaluation in Education and the Social Sciences'. *Allyn and Bacon*.

Sonja Utz, Uwe Matzat, and Chris Snijders (2009). On-line Reputation Systems: The Effects of Feed-back Comments and Reactions on Building and Rebuilding Trust in On-line Auctions, *International Journal of Electronic Commerce*, Vol. 13, No. 3, pp: 95-118.

So, M.W.C. and Sculli, D. (2002). 'The Role of Trust, Quality, Value and Risk in Conducting e-Business', *Industrial Management and Data Systems*, Vol. 102, No. 9, pp. 503–512.

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

Spiekermann, S., Grossklags, J., and Berendt, B. (2001). 'E-privacy in 2ndgeneration e-commerce: Privacy preferences versus actual behavior.' In *Proceedings of the ACM conference on electronic commerce (EC'01), Tampa, FL,* pp. 38-47.

Sproull, N. L. (1995). 'Handbook of research methods: a guide to practitioners and the students in social sciences'. *The Scarecrow press Inc*.

Stephen Marsh and John Meech (2000). Trust in design. In *CHI 2000*, pp. 45 – 46.

Stewart, K. A., and Segars, A. H. (2002). "An Empirical Examination of the Concern for Information Privacy Instrument." *Information Systems Research*, Vol. 13, No. 1, pp. 36-49.

Suh, B., and Han, I. (2003). 'The impact of customer trust and perception of security control on the acceptance of electronic commerce', *International Journal of Electronic Commerce*, Vol. 7, No. 3, pp.135-161.

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

Swaminathan, V. et al. (December 1999). 'Browsers or Buyers in Cyberspace? An Investigation of Factors Influencing Electronic Exchange'. *Journal of Computer Mediated Communication*, Vol. 5, No. 2, pp. 1-10.

Syed Mahbubur, Rahman and Raisinghani, Mahesh S. (2000). Electronic Commerce: Opportunity and Challenges. *Idea Group Publishing*.

Szuprowics, Bohdan. (1998) 'Extranets and intranets: E-commerce Business Strategies for the Future'. *Computer Technology Research.*

Tamura, S. (2003) 'Future of the Internet Cyber Security'. *Global Business Dialogue on Electronic Commerce*, 27-31. [Online]. Available: http://www.docstoc.com/docs/2597936/Future-of-the-Internet-Cyber-Security.

Tan, S. J. (1999). Strategies for reducing consumers risk aversion in Internet shopping. *Journal of Consumer Marketing*, Vol. 16, No. 2, pp. 163-180.

Tan, F. B. and Sutherland, P. (2004). 'Online Consumer Trust: A Multi-Dimensional Model', *Journal of Electronic Commerce in Organizations*, Vol. 2, No. 3, pp. 40–58.

Tang, Fang-Fang, et al. (2003) 'Using Insurance To Create Trust On The Internet'. *Communications of the ACM*, Vol. 46, No. 12, pp. 337-344.

Tarte, Jeff. (2003, January 5). The need for Information Security in Today's Economy, [Online]. Available: http://sans.org/rr/papers/47/916.pdf.

The Federal-Provincial-Territorial Consumer Measures Committee. (2005) 'Identity Theft: Protect Your Business, Protect Your Customers'. [Online]. Available: http://cmcweb.ca/idtheft.

Thomson, I. (2005). 'Online Fraud Hits Record Levels'. *RSA Conference in San Francisco*. [Online]. Available: http://www.vnunet.com/news

Timothy Bickmore and Justine Cassell, (March 31 - April 4 2001). Relational agents: A model and implementation of building user trust. *SIGCHI'01*, Vol. 3, No. 1, pp. 396 – 403.

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

Turban, E. and King, D., and Lang J. (2009). 'Introduction to Electronic Commerce'. 2nd Edn. *Upper Saddle River*, New Jersey: Pearson Prentice-Hall, Inc.

Turner, A. (2004, November 16). 'Crusty security no protection at all'. [Online]. Available: http://www.crime-research.org/news/16.11.2004/794/.

van der Heijden, H., Verhagen, T., and Creemers, M. (2003). 'Understanding Online Purchase Intentions: Contributions from Technology and Trust Perspectives.' *European Journal of Information Systems*, Vol. 12, No. 1, p. 41.

Vijayasarathy, L. R., (2004). "Predicting Consumer Intentions to use On-line Shopping: The case for an Augmented Technology Acceptance Model", *Information & Management*, Vol. 41, No. 6, pp. 747-762.

Ward, S., Bridges, K., and Chitty, B. (2005). Do incentives matter? An examination of online privacy concerns and willingness to provide personal and financial information. *Journal of Marketing Communications*, Vol. 11, No. 1, pp. 21-40.

Wang, H., Lee, M. K., and Wang, C. (1998). 'Consumer Privacy Concerns about Internet Marketing.' *Communications of the ACM*, Vol. 41, No. 3, pp. 63-70.

Wat F.K.T., Ngai. E.W.T., and Chong T.C.E., (2005) "Potential Risks to E-commerce Development Using Exploratory Factor Analysis", *International Journal of Services Technology & Management*, Vol. 6, No. 1, p. 55-71.

Weiers, R. M. (2002). Introduction to business statistics. 4th Edition. Belmont, CA. *Duxury Press*.

Weiquan Wang and Izak Benbasat (2008), Attributions of Trust in Decision Support Technologies: A Study of Recommendation Agents for E-Commerce, *Journal of Management Information Systems,* Vol. 24, No. 4, pp: 249–273.

Wilkinson, D. and Birmingham, P. (2003). 'Using Research Instruments – A Guide for Researchers' *RoutledgeFalmer*.

Wilsdon, J. (2001) 'Digital Futures: Living in a dot-com World' *Earthscan Pubs.*

Wilson, S. (2001) 'The Future of Business Documentation', [Online]. Available: http://www.managementfirst.com/e_business/articles.

Xiaowen Fang and Gavriel Salvendy (December 2003). Customercentered rules for design of e-commerce web sites. *Communications of the ACM*, Vol. 46, No. 12, pp. 332-336.

Xu, H., and Teo, H. H. (2004). 'Alleviating Consumer's Privacy Concern in Location-Based Services: A Psychological Control Perspective', *Proceedings of the Twenty-Fifth Annual International Conference on Information Systems (ICIS)*, Washington, D. C., United States, pp. 793-806.

Yang, Z., and Jun, M. (2002). "Consumer Perception of E-service Quality: From Internet Purchaser and Non-purchaser Perspectives." *Journal of Business Strategies*, Vol. 19, No. 1, pp. 19-41.

Yao-Hua Tan and Walter Thoen (2000). Formal aspects of a generic model of trust for electronic commerce. In *Proceedings of the 33rd Hawaii International Conference on System Sciences*, pp. 1-8. IEEE.

Yee, L. H. and Seong, L. K., (Saturday April 11, 2009) "Buying via Internet", [Online]. Available: http://biz.thestar.com.my/news/story.asp?file=/2009/4/11/business/3620542.

Yousafzai, S.Y., Pallister, J.G., Foxall, G.R. (2003), "A proposed model of e-trust for electronic banking", *Technovation*, Vol. 23 No.11, pp. 847-60.

Yusof Ismail and Mohd Yusof Ishak (January 2005) "Driving forces and impediments to e-commerce activities among SMEs in Kuala Lumpur and Selangor," *Paper presented at Internationa Conference on E-commerce 2005,* The Summit Hotel, Kuala Lumpur.

Zikmund, K.G. (1999). Essentials of marketing research. *Harcourt brace and company*: Florida.

# PUBLICATIONS

1. Thaw, Y. Yi; Ahmad Kamil, Mahmood; and Dominic P, Dhanapal Durai. (2008). Consumers' Trust in E-Commerce Transactions: The Role of Perceived Security, Perceived Privacy, and Perceived Risk in the Context of E-commerce. Presented at *National Postgraduate Conference (NPC 2008)*, Universiti Teknologi PETRONAS.
2. Thaw, Y. Yi; Ahmad Kamil, Mahmood; and Dominic P, Dhanapal Durai. (2009). A Study on the Factors That Influence the Consumers' Trust on E-commerce Adoption. *International Journal of Computer Science and Information Security (IJCSIS)*, Vol.4, No. (1&2). pp. 153-159.
3. Thaw, Y. Yi; Ahmad Kamil, Mahmood; and Dominic P, Dhanapal Durai. (2010). Factors Influencing Consumers' Trust in E-commerce Transactions, Accepted at *The 2010 International Conference on Innovation and Management (IAM 2010),* Penang, Malaysia, July 7- 10, 2010.
4. Thaw, Y. Yi; Ahmad Kamil, Mahmood and Dominic P, Dhanapal Durai. (2010). Factors Associating Consumers' Trust in E-commerce Transactions, Accepted at *International Conference on Industrial Engineering and Business Management (ICIEBM) 2010,* Yogyakarta, 12-13 October 2010.
5. Thaw, Y. Yi; Dominic P, Dhanapal Durai and Ahmad Kamil, Mahmood. (2011). A Structural Equation Modeling Approach for Malaysian Consumers' Perspectives on E-commerce B2C Transactions. *International Journal of Business Innovation and Research (IJBIR),* (Under Review).
6. Thaw, Y. Yi; Dominic P, Dhanapal Durai and Ahmad Kamil, Mahmood. (2011). Factors Influencing Consumers' Trust in E-commerce Transactions: Malaysian Consumers' Perspectives. *International Journal of Business Information Systems (IJBIS),* (Under Review).

Appendix A

Research Questionnaire

A survey on "*CONSUMERS' TRUST IN E-COMMERCE TRANSACTIONS: The Role of Perceived Security, Perceived Privacy, and Perceived Risk in the Context of E-Commerce*".

You are invited to participate in a study of e-commerce as part of our research project for Universiti Teknologi PETRONAS, Malaysia (UTP). Your response to the questionnaire will be treated with utmost confidentiality and they will be used solely for academic purposes and none of the respondents will be identified in this study in any manner whatsoever.

SECTION 1

Please answer all the questions by ticking your answers in the suitable space.
Please choose only one option that describes you best.

1. Gender
   1) Male 2) Female

2. Age
   1) 20 years to 30 years 2) 31 years to 40 years
   3) 41 years to 50 years 4) Over 50 years

3. Race
   1) Malay 2) Chinese 3) Indian 4) Other

4. Education Level
   1) High School 2) Diploma 3) Degree
   4) Master 5) Ph.D Other

5. Primary Occupation
   1) Administrative Support 2) Management 3) Educator
   4) Sales Personnel 5) Professional 6) Other

SECTION 2

Please answer all the questions by ticking your answers in the suitable space.
Please choose only one option that describes you best.

6. How often do you use the Internet?
   1) Always 2) Sometimes 3) Seldom 4) Never

7. How often do you make online purchases from Web-based vendors? If your response is *'Never'*, please go to question 7(c).
1) Always 2) Sometimes 3) Seldom 4) Never

7(a). If you *have done* online purchasing, for how long have you been doing this?
1) Less than 1 year 2) 1-3 years
3) 4-6 years 4) More than 6 years

7(b). If you *have done* online purchasing, how many times do you think you will be doing this in the next six months compared to the previous six months?
1) I will not do this 2) Somewhat less
3) About the same 4) Somewhat more
5) Much more

7(c). If you *have not done* online purchasing, how likely is it that you will do this type of purchasing in the next six months?
1) I will not do this 2) Somewhat less
3) About the same 4) Somewhat more
5) Much more

7(d). If you *have not done* online purchasing and you *will not do* this type of purchasing in near future, what is the reason for not buying online?
1) Security/Privacy 2) Lack of time
3) Lack of interaction 4) Can't feel product
5) High prices 6) Other

8. What is your opinion on online credit card security?
1) Very Unsafe 2) Somewhat Unsafe
3) Indifferent 4) Somewhat Safe
5) Very Safe 6) Don't know

SECTION 3

Please indicate your degree of agreement or disagreement on all of the statements by circling the appropriate number on the 5-point scale given below that best describes how you feel about the statement.

1) Strongly disagree 2) Disagree 3) Neutral
4) Agree 5) Strongly agree

Perceived Information Security

| | | |
|---|---|---|
| 1 | I would feel totally safe providing sensitive information about myself over the Web. | 1 2 3 4 5 |
| 2 | I would believe the payment information I enter online is safe and accessible only by the intended recipient. | 1 2 3 4 5 |

| | | |
|---|---|---|
| 3 | I would believe the information I enter online is not altered in transit. | 1 2 3 4 5 |
| 4 | I would not hesitate to make purchase from the Web because of security issues of sensitive information. | 1 2 3 4 5 |
| 5 | Overall, I would believe that there is an adequate control in place to ensure security of personal data transmitted during online transaction processing. | 1 2 3 4 5 |

Perceived Information Privacy

| | | |
|---|---|---|
| 6 | My personal information would not be misused when transacting with online companies. | 1 2 3 4 5 |
| 7 | I believe I have control over how the information I provide will be used by online companies. | 1 2 3 4 5 |
| 8 | I believe I can later verify the information I provide during a transaction with online companies. | 1 2 3 4 5 |
| 9 | I believe that online companies will not reveal my sensitive information without my consent. | 1 2 3 4 5 |
| 10 | I believe there is an effective mechanism to address any violation of the sensitive information I provide to online companies. | 1 2 3 4 5 |
| 11 | I believe that there is an adequate control in place to protect the privacy of personal information within online companies. | 1 2 3 4 5 |

Trustworthiness of Web Vendors

| | | |
|---|---|---|
| 12 | I believe that online companies will act with high business standards. | 1 2 3 4 5 |
| 13 | Online companies have the skills and expertise to perform transactions in an expected manner. | 1 2 3 4 5 |
| 14 | I believe that online companies are dependable. | 1 2 3 4 5 |
| 15 | I believe that online companies do not have ill intentions about any of their consumers. | 1 2 3 4 5 |
| 16 | Overall, online companies are trustworthy. | 1 2 3 4 5 |

Perceived Risk

| | | |
|---|---|---|
| 17 | Providing credit card information over the Web is unsafe. | 1 2 3 4 5 |
| 18 | It would be risky to give personal information to online companies. | 1 2 3 4 5 |
| 19 | There would be too much uncertainty associated with providing personal information to online companies. | 1 2 3 4 5 |

Economic Incentives

| | | |
|---|---|---|
| 20 | Providing credit card information over the Web would not matter much if the prices were considerably lower. | 1 2 3 4 5 |
| 21 | Providing credit card information over the Web would not matter much if the products/services were of a higher quality. | 1 2 3 4 5 |

Institutional Trust

| | | |
|---|---|---|
| 22 | I would trust to open financial account, with *a Bank* (e.g., May bank, etc.), to facilitate transactions over the Internet. | 1 2 3 4 5 |
| 23 | I would trust to open financial account, with *a major credit card company* (e.g., MasterCard, Visa Card, etc.), to facilitate transactions over the Internet. | 1 2 3 4 5 |

Consumers' Trust

| | | |
|---|---|---|
| 24 | My confidence to adopt e-commerce will be more when online companies provide all necessary guaranties for security and privacy concern. | 1 2 3 4 5 |
| 25 | My confidence to purchase online will be more when more complex and advanced method is used for security and privacy concern. | 1 2 3 4 5 |

Thank you for your time. We appreciate your participation.

Online Survey Link:

http://www.freesurveysonline.com/fso/AskSurvey.fso?Survey=17324&CheckID=14848

Appendix B

Interview Questions

In order to know more about consumers' views on their perceptions related to e-commerce transactions, this set of questionnaire is used in the interview with individual consumer.

1) Have you ordered/paid anything online? If so, for what kind of products/services?
2) Would you usually like to test an online shop before actually buying from it?
3) What do you think about online services that need a kind of registration to gather your personal information?
4) Do you give your correct personal information to online companies?
5) What do you think about an online shop/service that has a link to bank services and you can pay it there besides well-known major credit card?
6) What do you think about providing financial or economic incentives by online store sites?
7) What do you think about giving credit card number and personal information to foreign online companies?

Appendix C

Descriptive Analysis

## Study I

**Gender**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Male | 43 | 50.6 | 50.6 | 50.6 |
| | Female | 42 | 49.4 | 49.4 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

**Age**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | 20-30 | 84 | 98.8 | 98.8 | 98.8 |
| | 31-40 | 1 | 1.2 | 1.2 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

**Race**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Malay | 49 | 57.6 | 57.6 | 57.6 |
| | Chinese | 16 | 18.8 | 18.8 | 76.5 |
| | Indian | 13 | 15.3 | 15.3 | 91.8 |
| | Other | 7 | 8.2 | 8.2 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

**Use of Internet**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Always | 73 | 85.9 | 85.9 | 85.9 |
| | Sometimes | 9 | 10.6 | 10.6 | 96.5 |
| | Seldom | 3 | 3.5 | 3.5 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

**N, Intension to purchase**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | I do not do this | 42 | 49.4 | 49.4 | 49.4 |
| | Somewhat less | 19 | 22.4 | 22.4 | 71.8 |
| | About the same | 17 | 20.0 | 20.0 | 91.8 |
| | Somewhat more | 6 | 7.1 | 7.1 | 98.8 |
| | Much more | 1 | 1.2 | 1.2 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

**N, Reason for not buying online**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Security/Privacy | 31 | 36.5 | 36.5 | 36.5 |
| | Lack of time | 7 | 8.2 | 8.2 | 44.7 |
| | Lack of interaction | 23 | 27.1 | 27.1 | 71.8 |
| | Can't feel product | 19 | 22.4 | 22.4 | 94.1 |
| | High prices | 2 | 2.4 | 2.4 | 96.5 |
| | Other | 3 | 3.5 | 3.5 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

**Opinion on Credit Card security**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Very Unsafe | 22 | 25.9 | 25.9 | 25.9 |
| | Somewhat Unsafe | 24 | 28.2 | 28.2 | 54.1 |
| | Indifferent | 7 | 8.2 | 8.2 | 62.4 |
| | Somewhat Safe | 10 | 11.8 | 11.8 | 74.1 |
| | Very Safe | 1 | 1.2 | 1.2 | 75.3 |
| | Don't know | 21 | 24.7 | 24.7 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

## Perceived Information Security

**Statistics**

| | | Feel safe providing info over Web | Accessible only by intended recipient | Info is not altered in transit | Not hesitate to purchase for security issues | Adequate control to ensure security |
|---|---|---|---|---|---|---|
| N | Valid | 85 | 85 | 85 | 85 | 85 |
| | Missing | 0 | 0 | 0 | 0 | 0 |
| Mean | | 2.31 | 2.73 | 2.73 | 2.66 | 2.96 |
| Std. Deviation | | .939 | .905 | .746 | .907 | .879 |

**Feel safe providing info over Web**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Strongly disagree | 19 | 22.4 | 22.4 | 22.4 |
| | Disagree | 30 | 35.3 | 35.3 | 57.6 |
| | Neutral | 27 | 31.8 | 31.8 | 89.4 |
| | Agree | 9 | 10.6 | 10.6 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

**Accessible only by intended recipient**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Strongly disagree | 7 | 8.2 | 8.2 | 8.2 |
| | Disagree | 28 | 32.9 | 32.9 | 41.2 |
| | Neutral | 31 | 36.5 | 36.5 | 77.6 |
| | Agree | 19 | 22.4 | 22.4 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

**Info is not altered in transit**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Strongly disagree | 5 | 5.9 | 5.9 | 5.9 |
| | Disagree | 23 | 27.1 | 27.1 | 32.9 |
| | Neutral | 47 | 55.3 | 55.3 | 88.2 |
| | Agree | 10 | 11.8 | 11.8 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

**Not hesitate to purchase for security issues**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Strongly disagree | 10 | 11.8 | 11.8 | 11.8 |
| | Disagree | 24 | 28.2 | 28.2 | 40.0 |
| | Neutral | 36 | 42.4 | 42.4 | 82.4 |
| | Agree | 15 | 17.6 | 17.6 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

**Adequate control to ensure security**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Strongly disagree | 4 | 4.7 | 4.7 | 4.7 |
| | Disagree | 22 | 25.9 | 25.9 | 30.6 |
| | Neutral | 32 | 37.6 | 37.6 | 68.2 |
| | Agree | 27 | 31.8 | 31.8 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

## Perceived Information Privacy

**Statistics**

| | | Info would not be misused | Control over how info will be used | Later verify info | Companies will not reveal info | Effective mechanism to address violation | Adequate control to ensure privacy |
|---|---|---|---|---|---|---|---|
| N | Valid | 85 | 85 | 85 | 85 | 85 | 85 |
| | Missing | 0 | 0 | 0 | 0 | 0 | 0 |
| Mean | | 3.08 | 3.13 | 3.02 | 2.87 | 3.13 | 3.12 |
| Std. Deviation | | .862 | .897 | .845 | .897 | .910 | .822 |

**Info would not be misused**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Strongly disagree | 4 | 4.7 | 4.7 | 4.7 |
| | Disagree | 16 | 18.8 | 18.8 | 23.5 |
| | Neutral | 34 | 40.0 | 40.0 | 63.5 |
| | Agree | 31 | 36.5 | 36.5 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

**Control over how info will be used**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Strongly disagree | 4 | 4.7 | 4.7 | 4.7 |
| | Disagree | 17 | 20.0 | 20.0 | 24.7 |
| | Neutral | 28 | 32.9 | 32.9 | 57.6 |
| | Agree | 36 | 42.4 | 42.4 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

**Later verify info**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Strongly disagree | 4 | 4.7 | 4.7 | 4.7 |
| | Disagree | 17 | 20.0 | 20.0 | 24.7 |
| | Neutral | 37 | 43.5 | 43.5 | 68.2 |
| | Agree | 27 | 31.8 | 31.8 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

**Companies will not reveal info**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Strongly disagree | 7 | 8.2 | 8.2 | 8.2 |
| | Disagree | 19 | 22.4 | 22.4 | 30.6 |
| | Neutral | 37 | 43.5 | 43.5 | 74.1 |
| | Agree | 22 | 25.9 | 25.9 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

**Effective mechanism to address violation**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Strongly disagree | 5 | 5.9 | 5.9 | 5.9 |
| | Disagree | 12 | 14.1 | 14.1 | 20.0 |
| | Neutral | 38 | 44.7 | 44.7 | 64.7 |
| | Agree | 27 | 31.8 | 31.8 | 96.5 |
| | Strongly agree | 3 | 3.5 | 3.5 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

**Adequate control to ensure privacy**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Strongly disagree | 4 | 4.7 | 4.7 | 4.7 |
| | Disagree | 12 | 14.1 | 14.1 | 18.8 |
| | Neutral | 39 | 45.9 | 45.9 | 64.7 |
| | Agree | 30 | 35.3 | 35.3 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

Trustworthiness of Web Vendors

**Statistics**

| | | Companies will act with high business standards | Companies have skills and expertise | Companies are dependable | Do not have ill intension about consumers | Companies are trustworthy |
|---|---|---|---|---|---|---|
| N | Valid | 85 | 85 | 85 | 85 | 85 |
| | Missing | 0 | 0 | 0 | 0 | 0 |
| Mean | | 3.06 | 3.21 | 3.02 | 2.89 | 2.88 |
| Std. Deviation | | .891 | .901 | .859 | .926 | .892 |

**Companies will act with high business standards**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Strongly disagree | 5 | 5.9 | 5.9 | 5.9 |
| | Disagree | 16 | 18.8 | 18.8 | 24.7 |
| | Neutral | 33 | 38.8 | 38.8 | 63.5 |
| | Agree | 31 | 36.5 | 36.5 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

**Companies have skills and expertise**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Strongly disagree | 4 | 4.7 | 4.7 | 4.7 |
| | Disagree | 15 | 17.6 | 17.6 | 22.4 |
| | Neutral | 25 | 29.4 | 29.4 | 51.8 |
| | Agree | 41 | 48.2 | 48.2 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

**Companies are dependable**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Strongly disagree | 4 | 4.7 | 4.7 | 4.7 |
| | Disagree | 17 | 20.0 | 20.0 | 24.7 |
| | Neutral | 38 | 44.7 | 44.7 | 69.4 |
| | Agree | 25 | 29.4 | 29.4 | 98.8 |
| | Strongly agree | 1 | 1.2 | 1.2 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

**Do not have ill intension about consumers**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Strongly disagree | 7 | 8.2 | 8.2 | 8.2 |
| | Disagree | 20 | 23.5 | 23.5 | 31.8 |
| | Neutral | 33 | 38.8 | 38.8 | 70.6 |
| | Agree | 25 | 29.4 | 29.4 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

**Companies are trustworthy**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Strongly disagree | 8 | 9.4 | 9.4 | 9.4 |
| | Disagree | 14 | 16.5 | 16.5 | 25.9 |
| | Neutral | 44 | 51.8 | 51.8 | 77.6 |
| | Agree | 18 | 21.2 | 21.2 | 98.8 |
| | Strongly agree | 1 | 1.2 | 1.2 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

Perceived Risk

**Statistics**

| | | Credit card info over Web is unsafe | Risky to give info | Uncertainty for providing info |
|---|---|---|---|---|
| N | Valid | 85 | 85 | 85 |
| | Missing | 0 | 0 | 0 |
| Mean | | 3.51 | 3.46 | 3.46 |
| Std. Deviation | | 1.031 | .894 | .946 |

**Credit card info over Web is unsafe**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Disagree | 16 | 18.8 | 18.8 | 18.8 |
| | Neutral | 28 | 32.9 | 32.9 | 51.8 |
| | Agree | 23 | 27.1 | 27.1 | 78.8 |
| | Strongly agree | 18 | 21.2 | 21.2 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

**Risky to give info**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Disagree | 15 | 17.6 | 17.6 | 17.6 |
| | Neutral | 24 | 28.2 | 28.2 | 45.9 |
| | Agree | 38 | 44.7 | 44.7 | 90.6 |
| | Strongly agree | 8 | 9.4 | 9.4 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

**Uncertainty for providing info**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Disagree | 16 | 18.8 | 18.8 | 18.8 |
| | Neutral | 25 | 29.4 | 29.4 | 48.2 |
| | Agree | 33 | 38.8 | 38.8 | 87.1 |
| | Strongly agree | 11 | 12.9 | 12.9 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

## Economic Incentives

**Statistics**

| | | Providing info not matter for low prices | Providing info not matter for higher quality |
|---|---|---|---|
| N | Valid | 85 | 85 |
| | Missing | 0 | 0 |
| Mean | | 2.91 | 3.14 |
| Std. Deviation | | .881 | .819 |

**Providing info not matter for low prices**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Disagree | 33 | 38.8 | 38.8 | 38.8 |
| | Neutral | 31 | 36.5 | 36.5 | 75.3 |
| | Agree | 17 | 20.0 | 20.0 | 95.3 |
| | Strongly agree | 4 | 4.7 | 4.7 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

**Providing info not matter for higher quality**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Disagree | 21 | 24.7 | 24.7 | 24.7 |
| | Neutral | 33 | 38.8 | 38.8 | 63.5 |
| | Agree | 29 | 34.1 | 34.1 | 97.6 |
| | Strongly agree | 2 | 2.4 | 2.4 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

## Institutional Trust

**Statistics**

| | | Trust to open account with a bank | Trust to open account with a credit card company |
|---|---|---|---|
| N | Valid | 85 | 85 |
| | Missing | 0 | 0 |
| Mean | | 3.54 | 3.45 |
| Std. Deviation | | .970 | .824 |

**Trust to open account with a bank**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Disagree | 15 | 17.6 | 17.6 | 17.6 |
| | Neutral | 23 | 27.1 | 27.1 | 44.7 |
| | Agree | 33 | 38.8 | 38.8 | 83.5 |
| | Strongly agree | 14 | 16.5 | 16.5 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

**Trust to open account with a credit card company**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Disagree | 7 | 8.2 | 8.2 | 8.2 |
| | Neutral | 44 | 51.8 | 51.8 | 60.0 |
| | Agree | 23 | 27.1 | 27.1 | 87.1 |
| | Strongly agree | 11 | 12.9 | 12.9 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

## Consumers' Trust

**Statistics**

| | | Confidence for complex and advanved method | Confidence for all necessary guaranties |
|---|---|---|---|
| N | Valid | 85 | 85 |
| | Missing | 0 | 0 |
| Mean | | 3.86 | 3.75 |
| Std. Deviation | | .966 | .925 |

**Confidence for complex and advanved method**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Disagree | 8 | 9.4 | 9.4 | 9.4 |
| | Neutral | 22 | 25.9 | 25.9 | 35.3 |
| | Agree | 29 | 34.1 | 34.1 | 69.4 |
| | Strongly agree | 26 | 30.6 | 30.6 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

**Confidence for all necessary guaranties**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Disagree | 7 | 8.2 | 8.2 | 8.2 |
| | Neutral | 28 | 32.9 | 32.9 | 41.2 |
| | Agree | 29 | 34.1 | 34.1 | 75.3 |
| | Strongly agree | 21 | 24.7 | 24.7 | 100.0 |
| | Total | 85 | 100.0 | 100.0 | |

## Study II

**Gender**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Male | 101 | 62.0 | 62.0 | 62.0 |
| | Female | 62 | 38.0 | 38.0 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

**Age**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | 20-30 | 132 | 81.0 | 81.0 | 81.0 |
| | 31-40 | 29 | 17.8 | 17.8 | 98.8 |
| | 41-50 | 2 | 1.2 | 1.2 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

**Race**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Malay | 88 | 54.0 | 54.0 | 54.0 |
| | Chinese | 38 | 23.3 | 23.3 | 77.3 |
| | Indian | 21 | 12.9 | 12.9 | 90.2 |
| | Other | 16 | 9.8 | 9.8 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

**Education Level**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | High School | 1 | .6 | .6 | .6 |
| | Diploma | 46 | 28.2 | 28.2 | 28.8 |
| | Degree | 88 | 54.0 | 54.0 | 82.8 |
| | Master | 28 | 17.2 | 17.2 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

**Primary Occupation**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Administrative Support | 35 | 21.5 | 21.5 | 21.5 |
| | Management | 75 | 46.0 | 46.0 | 67.5 |
| | Educator | 19 | 11.7 | 11.7 | 79.1 |
| | Sales Personnel | 23 | 14.1 | 14.1 | 93.3 |
| | Professional | 11 | 6.7 | 6.7 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

**Use of Internet**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Always | 158 | 96.9 | 96.9 | 96.9 |
| | Sometimes | 5 | 3.1 | 3.1 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

**Make online purchases**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Always | 1 | .6 | .6 | .6 |
| | Sometimes | 82 | 50.3 | 50.3 | 50.9 |
| | Seldom | 80 | 49.1 | 49.1 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

**How long have been purchasing**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Less than 1 year | 23 | 14.1 | 14.1 | 14.1 |
| | 1 to 3 years | 85 | 52.1 | 52.1 | 66.3 |
| | 4 to 6 years | 55 | 33.7 | 33.7 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

**Yes, Intension to purchase on Next**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Somewhat less | 3 | 1.8 | 1.8 | 1.8 |
| | About the same | 110 | 67.5 | 67.5 | 69.3 |
| | Somewhat more | 50 | 30.7 | 30.7 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

**Opinion on Credit Card security**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Somewhat Unsafe | 36 | 22.1 | 22.1 | 22.1 |
| | Indifferent | 25 | 15.3 | 15.3 | 37.4 |
| | Somewhat Safe | 98 | 60.1 | 60.1 | 97.5 |
| | Very Safe | 4 | 2.5 | 2.5 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

## Perceived Information Security

**Statistics**

| | | Feel safe providing info over Web | Accessible only by intended recipient | Info is not altered in transit | Not hesitate to purchase for security issues | Adequate control to ensure security |
|---|---|---|---|---|---|---|
| N | Valid | 163 | 163 | 163 | 163 | 163 |
| | Missing | 0 | 0 | 0 | 0 | 0 |
| Mean | | 3.58 | 3.79 | 3.64 | 3.75 | 3.79 |
| Std. Deviation | | .496 | .412 | .482 | .435 | .408 |

**Feel safe providing info over Web**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Neutral | 69 | 42.3 | 42.3 | 42.3 |
| | Agree | 94 | 57.7 | 57.7 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

**Accessible only by intended recipient**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Neutral | 35 | 21.5 | 21.5 | 21.5 |
| | Agree | 128 | 78.5 | 78.5 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

**Info is not altered in transit**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Neutral | 59 | 36.2 | 36.2 | 36.2 |
| | Agree | 104 | 63.8 | 63.8 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

**Not hesitate to purchase for security issues**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Neutral | 41 | 25.2 | 25.2 | 25.2 |
| | Agree | 122 | 74.8 | 74.8 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

**Adequate control to ensure security**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Neutral | 34 | 20.9 | 20.9 | 20.9 |
| | Agree | 129 | 79.1 | 79.1 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

## Perceived Information Privacy

**Statistics**

| | | nfo would not be misused | Control over how info will be used | Later verify info | Companies will not reveal info | Effective mechanism to address violation | Adequate control to ensure privacy |
|---|---|---|---|---|---|---|---|
| N | Valid | 163 | 163 | 163 | 163 | 163 | 163 |
| | Missing | 0 | 0 | 0 | 0 | 0 | 0 |
| Mean | | 3.47 | 3.37 | 3.80 | 3.45 | 3.60 | 3.71 |
| Std. Deviation | | .500 | .484 | .398 | .499 | .492 | .454 |

**Info would not be misused**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Neutral | 87 | 53.4 | 53.4 | 53.4 |
| | Agree | 76 | 46.6 | 46.6 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

**Control over how info will be used**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Neutral | 103 | 63.2 | 63.2 | 63.2 |
| | Agree | 60 | 36.8 | 36.8 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

**Later verify info**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Neutral | 32 | 19.6 | 19.6 | 19.6 |
| | Agree | 131 | 80.4 | 80.4 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

**Companies will not reveal info**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Neutral | 89 | 54.6 | 54.6 | 54.6 |
| | Agree | 74 | 45.4 | 45.4 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

**Effective mechanism to address violation**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Neutral | 66 | 40.5 | 40.5 | 40.5 |
| | Agree | 97 | 59.5 | 59.5 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

**Adequate control to ensure privacy**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Neutral | 47 | 28.8 | 28.8 | 28.8 |
| | Agree | 116 | 71.2 | 71.2 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

## Trustworthiness of Web Vendors

**Statistics**

| | | Companies will act with high business standards | Companies have skills and expertise | Companies are dependable | Do not have ill intension about consumers | Companies are trustworthy |
|---|---|---|---|---|---|---|
| N | Valid | 163 | 163 | 163 | 163 | 163 |
| | Missing | 0 | 0 | 0 | 0 | 0 |
| Mean | | 3.44 | 3.75 | 3.27 | 3.21 | 3.21 |
| Std. Deviation | | .498 | .435 | .445 | .412 | .412 |

**Companies will act with high business standards**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Neutral | 91 | 55.8 | 55.8 | 55.8 |
| | Agree | 72 | 44.2 | 44.2 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

**Companies have skills and expertise**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Neutral | 41 | 25.2 | 25.2 | 25.2 |
| | Agree | 122 | 74.8 | 74.8 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

**Companies are dependable**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Neutral | 119 | 73.0 | 73.0 | 73.0 |
| | Agree | 44 | 27.0 | 27.0 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

**Do not have ill intension about consumers**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Neutral | 128 | 78.5 | 78.5 | 78.5 |
| | Agree | 35 | 21.5 | 21.5 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

**Companies are trustworthy**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Neutral | 128 | 78.5 | 78.5 | 78.5 |
| | Agree | 35 | 21.5 | 21.5 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

Perceived Risk

**Statistics**

| | | Credit card info over Web is unsafe | Risky to give info | Uncertainty for providing info |
|---|---|---|---|---|
| N | Valid | 163 | 163 | 163 |
| | Missing | 0 | 0 | 0 |
| Mean | | 3.86 | 4.06 | 3.81 |
| Std. Deviation | | .383 | .328 | .539 |

**Credit card info over Web is unsafe**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Neutral | 25 | 15.3 | 15.3 | 15.3 |
| | Agree | 136 | 83.4 | 83.4 | 98.8 |
| | Strongly agree | 2 | 1.2 | 1.2 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

**Risky to give info**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Neutral | 4 | 2.5 | 2.5 | 2.5 |
| | Agree | 145 | 89.0 | 89.0 | 91.4 |
| | Strongly agree | 14 | 8.6 | 8.6 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

**Uncertainty for providing info**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Neutral | 42 | 25.8 | 25.8 | 25.8 |
| | Agree | 110 | 67.5 | 67.5 | 93.3 |
| | Strongly agree | 11 | 6.7 | 6.7 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

Economic Incentives

**Statistics**

| | | Providing info not matter for low prices | Providing info not matter for higher quality |
|---|---|---|---|
| N | Valid | 163 | 163 |
| | Missing | 0 | 0 |
| Mean | | 3.46 | 3.83 |
| Std. Deviation | | .524 | .439 |

**Providing info not matter for low prices**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Disagree | 2 | 1.2 | 1.2 | 1.2 |
| | Neutral | 84 | 51.5 | 51.5 | 52.8 |
| | Agree | 77 | 47.2 | 47.2 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

**Providing info not matter for higher quality**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Neutral | 32 | 19.6 | 19.6 | 19.6 |
| | Agree | 127 | 77.9 | 77.9 | 97.5 |
| | Strongly agree | 4 | 2.5 | 2.5 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

Institutional Trust

**Statistics**

| | | Trust to open account with a bank | Trust to open account with a credit card company |
|---|---|---|---|
| N | Valid | 163 | 163 |
| | Missing | 0 | 0 |
| Mean | | 3.46 | 4.52 |
| Std. Deviation | | .500 | .501 |

**Trust to open account with a bank**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Neutral | 88 | 54.0 | 54.0 | 54.0 |
| | Agree | 75 | 46.0 | 46.0 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

**Trust to open account with a credit card company**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Agree | 79 | 48.5 | 48.5 | 48.5 |
| | Strongly agree | 84 | 51.5 | 51.5 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

Consumers' Trust

**Statistics**

| | | Confidence for complex and advanved method | Confidence for all necessary guaranties |
|---|---|---|---|
| N | Valid | 163 | 163 |
| | Missing | 0 | 0 |
| Mean | | 3.74 | 4.30 |
| Std. Deviation | | .456 | .473 |

**Confidence for complex and advanved method**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Neutral | 44 | 27.0 | 27.0 | 27.0 |
| | Agree | 118 | 72.4 | 72.4 | 99.4 |
| | Strongly agree | 1 | .6 | .6 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

**Confidence for all necessary guaranties**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Neutral | 1 | .6 | .6 | .6 |
| | Agree | 112 | 68.7 | 68.7 | 69.3 |
| | Strongly agree | 50 | 30.7 | 30.7 | 100.0 |
| | Total | 163 | 100.0 | 100.0 | |

## Overall Study

**Gender**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Male | 144 | 58.1 | 58.1 | 58.1 |
| | Female | 104 | 41.9 | 41.9 | 100.0 |
| | Total | 248 | 100.0 | 100.0 | |

**Age**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | 20-30 | 216 | 87.1 | 87.1 | 87.1 |
| | 31-40 | 30 | 12.1 | 12.1 | 99.2 |
| | 41-50 | 2 | .8 | .8 | 100.0 |
| | Total | 248 | 100.0 | 100.0 | |

**Race**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Malay | 137 | 55.2 | 55.2 | 55.2 |
| | Chinese | 54 | 21.8 | 21.8 | 77.0 |
| | Indian | 34 | 13.7 | 13.7 | 90.7 |
| | Other | 23 | 9.3 | 9.3 | 100.0 |
| | Total | 248 | 100.0 | 100.0 | |

**Use of Internet**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Always | 231 | 93.1 | 93.1 | 93.1 |
| | Sometimes | 14 | 5.6 | 5.6 | 98.8 |
| | Seldom | 3 | 1.2 | 1.2 | 100.0 |
| | Total | 248 | 100.0 | 100.0 | |

**Opinion on Credit Card security**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Very Unsafe | 22 | 8.9 | 8.9 | 8.9 |
| | Somewhat Unsafe | 60 | 24.2 | 24.2 | 33.1 |
| | Indifferent | 32 | 12.9 | 12.9 | 46.0 |
| | Somewhat Safe | 108 | 43.5 | 43.5 | 89.5 |
| | Very Safe | 5 | 2.0 | 2.0 | 91.5 |
| | Don't know | 21 | 8.5 | 8.5 | 100.0 |
| | Total | 248 | 100.0 | 100.0 | |

## Perceived Information Security

**Not hesitate to purchase for security issues**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Strongly disagree | 10 | 4.0 | 4.0 | 4.0 |
| | Disagree | 38 | 15.3 | 15.3 | 19.4 |
| | Neutral | 89 | 35.9 | 35.9 | 55.2 |
| | Agree | 111 | 44.8 | 44.8 | 100.0 |
| | Total | 248 | 100.0 | 100.0 | |

**Adequate control to ensure security**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Strongly disagree | 4 | 1.6 | 1.6 | 1.6 |
| | Disagree | 23 | 9.3 | 9.3 | 10.9 |
| | Neutral | 56 | 22.6 | 22.6 | 33.5 |
| | Agree | 164 | 66.1 | 66.1 | 99.6 |
| | Strongly agree | 1 | .4 | .4 | 100.0 |
| | Total | 248 | 100.0 | 100.0 | |

## Perceived Information Privacy

**Later verify info**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Strongly disagree | 4 | 1.6 | 1.6 | 1.6 |
| | Disagree | 18 | 7.3 | 7.3 | 8.9 |
| | Neutral | 49 | 19.8 | 19.8 | 28.6 |
| | Agree | 160 | 64.5 | 64.5 | 93.1 |
| | Strongly agree | 17 | 6.9 | 6.9 | 100.0 |
| | Total | 248 | 100.0 | 100.0 | |

**Effective mechanism to address violation**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Strongly disagree | 5 | 2.0 | 2.0 | 2.0 |
| | Disagree | 12 | 4.8 | 4.8 | 6.9 |
| | Neutral | 103 | 41.5 | 41.5 | 48.4 |
| | Agree | 124 | 50.0 | 50.0 | 98.4 |
| | Strongly agree | 4 | 1.6 | 1.6 | 100.0 |
| | Total | 248 | 100.0 | 100.0 | |

**Adequate control to ensure privacy**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Strongly disagree | 4 | 1.6 | 1.6 | 1.6 |
| | Disagree | 13 | 5.2 | 5.2 | 6.9 |
| | Neutral | 66 | 26.6 | 26.6 | 33.5 |
| | Agree | 165 | 66.5 | 66.5 | 100.0 |
| | Total | 248 | 100.0 | 100.0 | |

## Trustworthiness of Web Vendors

**Companies will act with high business standards**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Strongly disagree | 5 | 2.0 | 2.0 | 2.0 |
| | Disagree | 16 | 6.5 | 6.5 | 8.5 |
| | Neutral | 104 | 41.9 | 41.9 | 50.4 |
| | Agree | 123 | 49.6 | 49.6 | 100.0 |
| | Total | 248 | 100.0 | 100.0 | |

**Companies have skills and expertise**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Strongly disagree | 4 | 1.6 | 1.6 | 1.6 |
| | Disagree | 15 | 6.0 | 6.0 | 7.7 |
| | Neutral | 62 | 25.0 | 25.0 | 32.7 |
| | Agree | 166 | 66.9 | 66.9 | 99.6 |
| | Strongly agree | 1 | .4 | .4 | 100.0 |
| | Total | 248 | 100.0 | 100.0 | |

Perceived Risk

**Credit card info over Web is unsafe**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Disagree | 17 | 6.9 | 6.9 | 6.9 |
| | Neutral | 65 | 26.2 | 26.2 | 33.1 |
| | Agree | 135 | 54.4 | 54.4 | 87.5 |
| | Strongly agree | 31 | 12.5 | 12.5 | 100.0 |
| | Total | 248 | 100.0 | 100.0 | |

**Uncertainty for providing info**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Disagree | 16 | 6.5 | 6.5 | 6.5 |
| | Neutral | 50 | 20.2 | 20.2 | 26.6 |
| | Agree | 155 | 62.5 | 62.5 | 89.1 |
| | Strongly agree | 27 | 10.9 | 10.9 | 100.0 |
| | Total | 248 | 100.0 | 100.0 | |

Economic Incentive

**Providing info not matter for low prices**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Disagree | 1 | .4 | .4 | .4 |
| | Neutral | 67 | 27.0 | 27.0 | 27.4 |
| | Agree | 156 | 62.9 | 62.9 | 90.3 |
| | Strongly agree | 24 | 9.7 | 9.7 | 100.0 |
| | Total | 248 | 100.0 | 100.0 | |

**Providing info not matter for higher quality**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Disagree | 4 | 1.6 | 1.6 | 1.6 |
| | Neutral | 66 | 26.6 | 26.6 | 28.2 |
| | Agree | 166 | 66.9 | 66.9 | 95.2 |
| | Strongly agree | 12 | 4.8 | 4.8 | 100.0 |
| | Total | 248 | 100.0 | 100.0 | |

Institutional Trust

**Trust to open account with a bank**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Disagree | 10 | 4.0 | 4.0 | 4.0 |
| | Neutral | 67 | 27.0 | 27.0 | 31.0 |
| | Agree | 159 | 64.1 | 64.1 | 95.2 |
| | Strongly agree | 12 | 4.8 | 4.8 | 100.0 |
| | Total | 248 | 100.0 | 100.0 | |

**Trust to open account with a credit card company**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Disagree | 1 | .4 | .4 | .4 |
| | Neutral | 27 | 10.9 | 10.9 | 11.3 |
| | Agree | 56 | 22.6 | 22.6 | 33.9 |
| | Strongly agree | 164 | 66.1 | 66.1 | 100.0 |
| | Total | 248 | 100.0 | 100.0 | |

Consumers' Trust

**Confidence for complex and advanved method**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Disagree | 8 | 3.2 | 3.2 | 3.2 |
| | Neutral | 22 | 8.9 | 8.9 | 12.1 |
| | Agree | 48 | 19.4 | 19.4 | 31.5 |
| | Strongly agree | 170 | 68.5 | 68.5 | 100.0 |
| | Total | 248 | 100.0 | 100.0 | |

**Confidence for all necessary guaranties**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Disagree | 7 | 2.8 | 2.8 | 2.8 |
| | Neutral | 40 | 16.1 | 16.1 | 19.0 |
| | Agree | 78 | 31.5 | 31.5 | 50.4 |
| | Strongly agree | 123 | 49.6 | 49.6 | 100.0 |
| | Total | 248 | 100.0 | 100.0 | |

Appendix D

Reliability Analysis

**Study I**

```
****** Method 1 (space saver) will be used for this analysis ******
R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   (A L P H A)
                          Mean        Std Dev       Cases
  1.     SAFEINFO         2.3059          .9389        85.0
  2.     INTENREC         2.7294          .9049        85.0
  3.     NOTALTER         2.7294          .7462        85.0
  4.     NOTHESIT         2.6588          .9070        85.0
  5.     SECTRANS         2.9647          .8789        85.0
  6.     NOMISUSE         3.0824          .8621        85.0
  7.     CNTRINFO         3.1294          .8969        85.0
  8.     LATVINFO         3.0235          .8448        85.0
  9.     NORVINFO         2.8706          .8969        85.0
 10.     EFFEMECH         3.1294          .9101        85.0
 11.     PRIVINFO         3.1176          .8225        85.0
 12.     HIGHBSTD         3.0588          .8911        85.0
 13.     SKILEXPE         3.2118          .9010        85.0
 14.     CODEPEND         3.0235          .8588        85.0
 15.     NOILLINT         2.8941          .9261        85.0
 16.     COMTRUST         2.8824          .8919        85.0
 17.     CRUNSAFE         3.5059         1.0308        85.0
 18.     RISKGVIN         3.4588          .8938        85.0
 19.     UNCERTAN         3.4588          .9456        85.0
 20.     PRICELOW         2.9059          .8813        85.0
 21.     HIGHQUAL         3.1412          .8187        85.0
 22.     TRUSTBNK         3.5412          .9704        85.0
 23.     TRUCRCOM         3.4471          .8238        85.0
 24.     CONFIADV         3.8588          .9655        85.0
 25.     CONFIGUA         3.7529          .9246        85.0

Reliability Coefficients
N of Cases =     85.0                  N of Items = 25
Alpha =    .8198
```

<u>Perceived Information Security</u>

```
****** Method 1 (space saver) will be used for this analysis ******
R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   (A L P H A)
                           Mean        Std Dev       Cases
  1.     SAFEINFO         2.3059          .9389        85.0
  2.     INTENREC         2.7294          .9049        85.0
  3.     NOTALTER         2.7294          .7462        85.0
  4.     NOTHESIT         2.6588          .9070        85.0
  5.     SECTRANS         2.9647          .8789        85.0

Reliability Coefficients
N of Cases =     85.0                  N of Items =  5
Alpha =    .7248
```

## Perceived Information Privacy

```
****** Method 1 (space saver) will be used for this analysis ******

R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   (A L P H A)

                            Mean        Std Dev       Cases

  1.     NOMISUSE          3.0824          .8621        85.0
  2.     CNTRINFO          3.1294          .8969        85.0
  3.     LATVINFO          3.0235          .8448        85.0
  4.     NORVINFO          2.8706          .8969        85.0
  5.     EFFEMECH          3.1294          .9101        85.0
  6.     PRIVINFO          3.1176          .8225        85.0

Reliability Coefficients

N of Cases =     85.0                  N of Items =  6

Alpha =    .6364
```

## Trustworthiness of Web Vendors

```
 ****** Method 1 (space saver) will be used for this analysis ******

R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   (A L P H A)

                            Mean        Std Dev       Cases

  1.     HIGHBSTD          3.0588          .8911        85.0
  2.     SKILEXPE          3.2118          .9010        85.0
  3.     CODEPEND          3.0235          .8588        85.0
  4.     NOILLINT          2.8941          .9261        85.0
  5.     COMTRUST          2.8824          .8919        85.0

Reliability Coefficients

N of Cases =     85.0                  N of Items =  5

Alpha =    .6603
```

## Perceived Risk

```
 ****** Method 1 (space saver) will be used for this analysis ******

R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   (A L P H A)

                            Mean        Std Dev       Cases

  1.     CRUNSAFE          3.5059         1.0308        85.0
  2.     RISKGVIN          3.4588          .8938        85.0
  3.     UNCERTAN          3.4588          .9456        85.0

Reliability Coefficients

N of Cases =     85.0                  N of Items =  3

Alpha =    .6422
```

Economic Incentives

```
****** Method 1 (space saver) will be used for this analysis ******

R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   (A L P H A)

                            Mean        Std Dev       Cases

  1.     PRICELOW          2.9059          .8813        85.0
  2.     HIGHQUAL          3.1412          .8187        85.0

Reliability Coefficients

N of Cases =     85.0                    N of Items =  2

Alpha =    .6595
```

Institutional Trust

```
****** Method 1 (space saver) will be used for this analysis ******

R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   (A L P H A)

                            Mean        Std Dev       Cases

  1.     TRUSTBNK          3.5412          .9704        85.0
  2.     TRUCRCOM          3.4471          .8238        85.0

Reliability Coefficients

N of Cases =     85.0                    N of Items =  2

Alpha =    .7791
```

Consumers' Trust

```
****** Method 1 (space saver) will be used for this analysis ******

R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   (A L P H A)

                            Mean        Std Dev       Cases

  1.     CONFIADV          3.8588          .9655        85.0
  2.     CONFIGUA          3.7529          .9246        85.0

Reliability Coefficients

N of Cases =     85.0                    N of Items =  2

Alpha =    .7069
```

## Study II

****** Method 1 (space saver) will be used for this analysis ******

R E L I A B I L I T Y  A N A L Y S I S  -  S C A L E  (A L P H A)

| | | Mean | Std Dev | Cases |
|---|---|---|---|---|
| 1. | SAFEINFO | 3.5767 | .4956 | 163.0 |
| 2. | INTENREC | 3.7853 | .4119 | 163.0 |
| 3. | NOTALTER | 3.6380 | .4820 | 163.0 |
| 4. | NOTHESIT | 3.7485 | .4352 | 163.0 |
| 5. | SECTRANS | 3.7914 | .4076 | 163.0 |
| 6. | NOMISUSE | 3.4663 | .5004 | 163.0 |
| 7. | CNTRINFO | 3.3681 | .4838 | 163.0 |
| 8. | LATVINFO | 3.8037 | .3984 | 163.0 |
| 9. | NORVINFO | 3.4540 | .4994 | 163.0 |
| 10. | EFFEMECH | 3.5951 | .4924 | 163.0 |
| 11. | PRIVINFO | 3.7117 | .4544 | 163.0 |
| 12. | HIGHBSTD | 3.4417 | .4981 | 163.0 |
| 13. | SKILEXPE | 3.7485 | .4352 | 163.0 |
| 14. | CODEPEND | 3.2699 | .4453 | 163.0 |
| 15. | NOILLINT | 3.2147 | .4119 | 163.0 |
| 16. | COMTRUST | 3.2147 | .4119 | 163.0 |
| 17. | CRUNSAFE | 3.8589 | .3829 | 163.0 |
| 18. | RISKGVIN | 4.0613 | .3276 | 163.0 |
| 19. | UNCERTAN | 3.8098 | .5392 | 163.0 |
| 20. | PRICELOW | 3.4601 | .5241 | 163.0 |
| 21. | HIGHQUAL | 3.8282 | .4388 | 163.0 |
| 22. | TRUSTBNK | 3.4601 | .4999 | 163.0 |
| 23. | TRUCRCOM | 4.5153 | .5013 | 163.0 |
| 24. | CONFIADV | 3.7362 | .4558 | 163.0 |
| 25. | CONFIGUA | 4.3006 | .4732 | 163.0 |

Reliability Coefficients
N of Cases = 163.0 N of Items = 25
Alpha = .7714

Perceived Information Security

****** Method 1 (space saver) will be used for this analysis ******

R E L I A B I L I T Y  A N A L Y S I S  -  S C A L E  (A L P H A)

| | | Mean | Std Dev | Cases |
|---|---|---|---|---|
| 1. | SAFEINFO | 3.5767 | .4956 | 163.0 |
| 2. | INTENREC | 3.7853 | .4119 | 163.0 |
| 3. | NOTALTER | 3.6380 | .4820 | 163.0 |
| 4. | NOTHESIT | 3.7485 | .4352 | 163.0 |
| 5. | SECTRANS | 3.7914 | .4076 | 163.0 |

Reliability Coefficients

N of Cases = 163.0 N of Items = 5

Alpha = .7376

## Perceived Information Privacy

```
 ****** Method 1 (space saver) will be used for this analysis ******

R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   (A L P H A)

                            Mean        Std Dev       Cases

  1.     NOMISUSE          3.4663          .5004       163.0
  2.     CNTRINFO          3.3681          .4838       163.0
  3.     LATVINFO          3.8037          .3984       163.0
  4.     NORVINFO          3.4540          .4994       163.0
  5.     EFFEMECH          3.5951          .4924       163.0
  6.     PRIVINFO          3.7117          .4544       163.0

Reliability Coefficients

N of Cases =    163.0                   N of Items =  6

Alpha =    .7718
```

## Trustworthiness of Web Vendors

```
****** Method 1 (space saver) will be used for this analysis ******

R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   (A L P H A)

                            Mean        Std Dev       Cases

  1.     HIGHBSTD          3.4417          .4981       163.0
  2.     SKILEXPE          3.7485          .4352       163.0
  3.     CODEPEND          3.2699          .4453       163.0
  4.     NOILLINT          3.2147          .4119       163.0
  5.     COMTRUST          3.2147          .4119       163.0

Reliability Coefficients

N of Cases =    163.0                   N of Items =  5

Alpha =    .7776
```

## Perceived Risk

```
****** Method 1 (space saver) will be used for this analysis ******

R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   (A L P H A)

                            Mean        Std Dev       Cases

  1.     CRUNSAFE          3.8589          .3829       163.0
  2.     RISKGVIN          4.0613          .3276       163.0
  3.     UNCERTAN          3.8098          .5392       163.0

Reliability Coefficients

N of Cases =    163.0                   N of Items =  3

Alpha =    .6412
```

Economic Incentives

```
****** Method 1 (space saver) will be used for this analysis ******

R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   (A L P H A)

                            Mean        Std Dev       Cases

  1.     PRICELOW          3.4601          .5241       163.0
  2.     HIGHQUAL          3.8282          .4388       163.0

Reliability Coefficients

N of Cases =    163.0                   N of Items =  2

Alpha =    .6419
```

Institutional Trust

```
****** Method 1 (space saver) will be used for this analysis ******

R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   (A L P H A)

                            Mean        Std Dev       Cases

  1.     TRUSTBNK          3.4601          .4999       163.0
  2.     TRUCRCOM          4.5153          .5013       163.0

Reliability Coefficients

N of Cases =    163.0                   N of Items =  2

Alpha =    .6066
```

Consumers' Trust

```
****** Method 1 (space saver) will be used for this analysis ******

R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   (A L P H A)

                            Mean        Std Dev       Cases

  1.     CONFIADV          3.7362          .4558       163.0
  2.     CONFIGUA          4.3006          .4732       163.0

Reliability Coefficients

N of Cases =    163.0                   N of Items =  2

Alpha =    .6423
```

## Overall Study

```
****** Method 1 (space saver) will be used for this analysis ******

R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   (A L P H
A)

                            Mean        Std Dev       Cases

  1.     SAFEINFO          2.8710          .9262       248.0
  2.     INTENREC          3.3347          .8228       248.0
  3.     NOTALTER          3.0242          .7306       248.0
  4.     NOTHESIT          3.2137          .8481       248.0
  5.     SECTRANS          3.5444          .7352       248.0
  6.     NOMISUSE          3.2379          .6881       248.0
  7.     CNTRINFO          3.0766          .6957       248.0
  8.     LATVINFO          3.6774          .7746       248.0
  9.     NORVINFO          3.0282          .6063       248.0
 10.     EFFEMECH          3.4435          .7063       248.0
 11.     PRIVINFO          3.5806          .6685       248.0
 12.     HIGHBSTD          3.3911          .7001       248.0
 13.     SKILEXPE          3.5847          .6860       248.0
 14.     CODEPEND          3.2218          .6576       248.0
 15.     NOILLINT          2.8468          .6975       248.0
 16.     COMTRUST          3.0565          .6209       248.0
 17.     CRUNSAFE          3.7258          .7671       248.0
 18.     RISKGVIN          3.9234          .6898       248.0
 19.     UNCERTAN          3.7782          .7221       248.0
 20.     PRICELOW          3.8185          .5929       248.0
 21.     HIGHQUAL          3.7500          .5637       248.0
 22.     TRUSTBNK          3.6976          .6245       248.0
 23.     TRUCRCOM          4.5444          .7014       248.0
 24.     CONFIADV          4.5323          .7889       248.0
 25.     CONFIGUA          4.2782          .8340       248.0

Reliability Coefficients
N of Cases =    248.0                   N of Items = 25
Alpha =    .8760
```

## Perceived Information Security

```
****** Method 1 (space saver) will be used for this analysis ******

R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   (A L P H
A)

                            Mean        Std Dev       Cases

  1.     SAFEINFO          2.8710          .9262       248.0
  2.     INTENREC          3.3347          .8228       248.0
  3.     NOTALTER          3.0242          .7306       248.0
  4.     NOTHESIT          3.2137          .8481       248.0
  5.     SECTRANS          3.5444          .7352       248.0

Reliability Coefficients
N of Cases =    248.0                   N of Items =  5
Alpha =    .8184
```

## Perceived Information Privacy

```
****** Method 1 (space saver) will be used for this analysis ******

R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   (A L P H
A)

                            Mean        Std Dev       Cases

  1.     NOMISUSE          3.2379          .6881       248.0
  2.     CNTRINFO          3.0766          .6957       248.0
  3.     LATVINFO          3.6774          .7746       248.0
  4.     NORVINFO          3.0282          .6063       248.0
  5.     EFFEMECH          3.4435          .7063       248.0
  6.     PRIVINFO          3.5806          .6685       248.0

Reliability Coefficients
N of Cases =    248.0                   N of Items =  6
Alpha =    .7014
```

## Trustworthiness of Web Vendors

```
 ****** Method 1 (space saver) will be used for this analysis ******

R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   (A L P H
A)

                            Mean        Std Dev       Cases

  1.     HIGHBSTD          3.3911          .7001       248.0
  2.     SKILEXPE          3.5847          .6860       248.0
  3.     CODEPEND          3.2218          .6576       248.0
  4.     NOILLINT          2.8468          .6975       248.0
  5.     COMTRUST          3.0565          .6209       248.0

Reliability Coefficients
N of Cases =    248.0                   N of Items =  5
Alpha =    .7147
```

## Perceived Risk

```
 ****** Method 1 (space saver) will be used for this analysis ******

R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   (A L P H
A)

                            Mean        Std Dev       Cases

  1.     CRUNSAFE          3.7258          .7671       248.0
  2.     RISKGVIN          3.9234          .6898       248.0
  3.     UNCERTAN          3.7782          .7221       248.0

Reliability Coefficients
N of Cases =    248.0                   N of Items =  3
Alpha =    .7068
```

Economic Incentives

```
 ****** Method 1 (space saver) will be used for this analysis ******

_
  R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   (A L P H
A)

                            Mean        Std Dev       Cases

  1.     PRICELOW          3.8185          .5929       248.0
  2.     HIGHQUAL          3.7500          .5637       248.0

Reliability Coefficients
N of Cases =    248.0                   N of Items =  2
Alpha =    .6155
```

Institutional Trust

```
 ****** Method 1 (space saver) will be used for this analysis ******

_
  R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   (A L P H
A)

                            Mean        Std Dev       Cases

  1.     TRUSTBNK          3.6976          .6245       248.0
  2.     TRUCRCOM          4.5444          .7014       248.0

Reliability Coefficients
N of Cases =    248.0                   N of Items =  2
Alpha =    .7675
```

Consumers' Trust

```
 ****** Method 1 (space saver) will be used for this analysis ******

_
  R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   (A L P H
A)

                            Mean        Std Dev       Cases

  1.     CONFIADV          4.5323          .7889       248.0
  2.     CONFIGUA          4.2782          .8340       248.0

Reliability Coefficients
N of Cases =    248.0                   N of Items =  2
Alpha =    .7577
```

**Overall Study (After SEM)**

Perceived Information Security

```
****** Method 1 (space saver) will be used for this analysis ******
_
R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   (A L P H A)
                            Mean        Std Dev       Cases

  1.     NOTHESIT          3.2137          .8481       248.0
  2.     SECTRANS          3.5444          .7352       248.0

Reliability Coefficients
N of Cases =    248.0                   N of Items =  2
Alpha =    .6630
```

Perceived Information Privacy

```
****** Method 1 (space saver) will be used for this analysis ******
_
R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   (A L P H A)
                            Mean        Std Dev       Cases

  1.     LATVINFO          3.6774          .7746       248.0
  2.     EFFEMECH          3.4435          .7063       248.0
  3.     PRIVINFO          3.5806          .6685       248.0

Reliability Coefficients
N of Cases =    248.0                   N of Items =  3
Alpha =    .7464
```

Trustworthiness of Web Vendors

```
****** Method 1 (space saver) will be used for this analysis ******
_
R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   (A L P H A)
                            Mean        Std Dev       Cases

  1.     HIGHBSTD          3.3911          .7001       248.0
  2.     SKILEXPE          3.5847          .6860       248.0

Reliability Coefficients
N of Cases =    248.0                   N of Items =  2
Alpha =    .7507
```

Perceived Risk

```
****** Method 1 (space saver) will be used for this analysis ******
_
R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   (A L P H A)
                            Mean        Std Dev       Cases

  1.     CRUNSAFE          3.7258          .7671       248.0
  2.     UNCERTAN          3.7782          .7221       248.0

Reliability Coefficients
N of Cases =    248.0                   N of Items =  2
Alpha =    .6012
```

## Economic Incentives

```
 ****** Method 1 (space saver) will be used for this analysis ******

R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   (A L P H A)

                            Mean        Std Dev       Cases

  1.     PRICELOW          3.8185          .5929       248.0
  2.     HIGHQUAL          3.7500          .5637       248.0

Reliability Coefficients

N of Cases =    248.0                   N of Items =  2

Alpha =    .6155
```

## Institutional Trust

```
****** Method 1 (space saver) will be used for this analysis ******

R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   (A L P H A)

                            Mean        Std Dev       Cases

  1.     TRUSTBNK          3.6976          .6245       248.0
  2.     TRUCRCOM          4.5444          .7014       248.0

Reliability Coefficients

N of Cases =    248.0                   N of Items =  2

Alpha =    .7675
```

## Consumers' Trust

```
****** Method 1 (space saver) will be used for this analysis ******

R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   (A L P H A)

                            Mean        Std Dev       Cases

  1.     CONFIADV          4.5323          .7889       248.0
  2.     CONFIGUA          4.2782          .8340       248.0

Reliability Coefficients

N of Cases =    248.0                   N of Items =  2

Alpha =    .7577
```

Appendix E

Factor Analysis

## Study I

**Communalities**

| | Initial | Extraction |
|---|---|---|
| Feel safe providing info over Web | 1.000 | .567 |
| Accessible only by intended recipient | 1.000 | .546 |
| Info is not altered in transit | 1.000 | .717 |
| Not hesitate to purchase for security issues | 1.000 | .625 |
| Adequate control to ensure security | 1.000 | .520 |
| Info would not be misused | 1.000 | .485 |
| Control over how info will be used | 1.000 | .714 |
| Later verify info | 1.000 | .537 |
| Companies will not reveal info | 1.000 | .725 |
| Effective mechanism to address violation | 1.000 | .707 |
| Adequate control to ensure privacy | 1.000 | .617 |
| Companies will act with high business standards | 1.000 | .510 |
| Companies have skills and expertise | 1.000 | .747 |
| Companies are dependable | 1.000 | .552 |
| Do not have ill intension about consumers | 1.000 | .521 |
| Companies are trustworthy | 1.000 | .657 |
| Credit card info over Web is unsafe | 1.000 | .593 |
| Risky to give info | 1.000 | .677 |
| Uncertainty for providing info | 1.000 | .545 |
| Providing info not matter for low prices | 1.000 | .588 |
| Providing info not matter for higher quality | 1.000 | .783 |
| Trust to open account with a bank | 1.000 | .767 |
| Trust to open account with a credit card company | 1.000 | .782 |
| Confidence for complex and advanved method | 1.000 | .727 |
| Confidence for all necessary guaranties | 1.000 | .688 |

Extraction Method: Principal Component Analysis.

**Total Variance Explained**

| Component | Initial Eigenvalues | | | Extraction Sums of Squared Loadings | | | Rotation Sums of Squared Loadings | | |
|---|---|---|---|---|---|---|---|---|---|
| | Total | % of Variance | Cumulative % | Total | % of Variance | Cumulative % | Total | % of Variance | Cumulative % |
| 1 | 5.504 | 22.015 | 22.015 | 5.504 | 22.015 | 22.015 | 3.096 | 12.383 | 12.383 |
| 2 | 2.953 | 11.811 | 33.826 | 2.953 | 11.811 | 33.826 | 2.639 | 10.555 | 22.938 |
| 3 | 1.829 | 7.316 | 41.142 | 1.829 | 7.316 | 41.142 | 2.269 | 9.078 | 32.016 |
| 4 | 1.661 | 6.646 | 47.788 | 1.661 | 6.646 | 47.788 | 2.247 | 8.988 | 41.003 |
| 5 | 1.447 | 5.788 | 53.576 | 1.447 | 5.788 | 53.576 | 2.217 | 8.870 | 49.873 |
| 6 | 1.324 | 5.295 | 58.871 | 1.324 | 5.295 | 58.871 | 1.859 | 7.438 | 57.311 |
| 7 | 1.181 | 4.725 | 63.596 | 1.181 | 4.725 | 63.596 | 1.571 | 6.286 | 63.596 |
| 8 | .939 | 3.756 | 67.353 | | | | | | |
| 9 | .919 | 3.677 | 71.029 | | | | | | |
| 10 | .841 | 3.365 | 74.395 | | | | | | |
| 11 | .829 | 3.316 | 77.711 | | | | | | |
| 12 | .745 | 2.979 | 80.690 | | | | | | |
| 13 | .682 | 2.727 | 83.416 | | | | | | |
| 14 | .599 | 2.396 | 85.813 | | | | | | |
| 15 | .560 | 2.240 | 88.053 | | | | | | |
| 16 | .483 | 1.933 | 89.985 | | | | | | |
| 17 | .394 | 1.578 | 91.563 | | | | | | |
| 18 | .385 | 1.540 | 93.103 | | | | | | |
| 19 | .366 | 1.462 | 94.565 | | | | | | |
| 20 | .326 | 1.305 | 95.871 | | | | | | |
| 21 | .271 | 1.085 | 96.955 | | | | | | |
| 22 | .243 | .972 | 97.928 | | | | | | |
| 23 | .217 | .866 | 98.794 | | | | | | |
| 24 | .179 | .716 | 99.510 | | | | | | |
| 25 | .122 | .490 | 100.000 | | | | | | |

Extraction Method: Principal Component Analysis.

**Component Transformation Matrix**

| Component | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| 1 | .632 | .547 | .422 | .057 | .331 | -.082 | .063 |
| 2 | .077 | -.219 | -.171 | .689 | .446 | .489 | -.060 |
| 3 | -.299 | .312 | .386 | .426 | -.397 | .013 | -.570 |
| 4 | -.374 | .022 | .561 | -.262 | .091 | .593 | .342 |
| 5 | .218 | -.260 | .238 | .440 | -.516 | -.145 | .589 |
| 6 | -.516 | .024 | .178 | .238 | .486 | -.596 | .231 |
| 7 | -.226 | .698 | -.491 | .145 | -.154 | .161 | .387 |

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

**Component Matrix[a]**

| | Component | | | | | | |
|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Feel safe providing info over Web | .400 | -.235 | .065 | -.478 | -.026 | .303 | -.164 |
| Accessible only by intended recipient | .570 | -.336 | .110 | -.061 | .076 | .228 | .186 |
| Info is not altered in transit | .702 | -.214 | .237 | -.118 | -.287 | .038 | .158 |
| Not hesitate to purchase for security issues | .565 | -.069 | .111 | -.119 | -.298 | .024 | .431 |
| Adequate control to ensure security | .690 | .033 | -.185 | -.050 | -.051 | -.057 | -.032 |
| Info would not be misused | .523 | .048 | .346 | -.191 | -.088 | .211 | .014 |
| Control over how info wil be used | .257 | .092 | .317 | -.012 | .589 | .375 | -.229 |
| Later verify info | .514 | .182 | -.176 | -.294 | .148 | -.204 | -.243 |
| Companies will not revea info | .451 | -.517 | .207 | .258 | -.143 | -.060 | -.347 |
| Effective mechanism to address violation | .670 | .060 | -.356 | -.187 | .250 | -.173 | .013 |
| Adequate control to ensure privacy | .563 | -.253 | -.118 | .257 | .317 | -.011 | -.236 |
| Companies will act with high business standards | .646 | -.015 | .046 | .081 | .062 | -.259 | -.114 |
| Companies have skills and expertise | .628 | -.058 | .096 | -.229 | .112 | -.524 | -.019 |
| Companies are dependable | .531 | -.046 | .202 | .389 | -.006 | .125 | -.245 |
| Do not have ill intension about consumers | .417 | -.251 | .103 | .177 | .003 | -.036 | .490 |
| Companies are trustworthy | .424 | .105 | .377 | .480 | .123 | -.097 | .262 |
| Credit card info over Wel is unsafe | .021 | .606 | .421 | .170 | .078 | .092 | .065 |
| Risky to give info | -.040 | .574 | .260 | -.316 | .313 | .061 | .277 |
| Uncertainty for providing info | .173 | .584 | .157 | -.334 | .178 | .062 | -.052 |
| Providing info not matter for low prices | .411 | .141 | -.568 | -.052 | .156 | .140 | .172 |
| Providing info not matter for higher quality | .083 | -.110 | -.499 | .413 | .475 | .183 | .292 |
| Trust to open account wi a bank | .526 | .413 | -.381 | -.060 | -.356 | .210 | -.013 |
| Trust to open account wi a credit card company | .379 | .401 | -.267 | .211 | -.366 | .457 | -.138 |
| Confidence for complex and advanved method | .226 | .704 | .070 | .376 | -.124 | -.006 | -.141 |
| Confidence for all necessary guaranties | .177 | .615 | -.086 | .181 | -.116 | -.474 | -.008 |

Extraction Method: Principal Component Analysis.

a. 7 components extracted.

**Rotated Component Matrix[a]**

| | Component | | | | | | |
|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Feel safe providing info over Web | .269 | .180 | .094 | .051 | .144 | -.633 | -.170 |
| Accessible only by intended recipient | .181 | .534 | .273 | -.021 | .033 | -.363 | .142 |
| Info is not altered in transit | .283 | .687 | .219 | -.070 | .174 | -.185 | -.218 |
| Not hesitate to purchase for security issues | .188 | .735 | -.052 | .001 | .200 | -.052 | -.067 |
| Adequate control to ensure security | .538 | .300 | .179 | -.045 | .316 | -.036 | .074 |
| Info would not be misused | .171 | .417 | .249 | .274 | .186 | -.240 | -.230 |
| Control over how info wi be used | .066 | -.085 | .527 | .531 | -.087 | -.325 | .171 |
| Later verify info | .694 | -.034 | .071 | .138 | .156 | -.069 | -.033 |
| Companies will not reve info | .165 | .223 | .629 | -.438 | -.042 | -.134 | -.202 |
| Effective mechanism to address violation | .745 | .178 | .052 | .047 | .158 | -.072 | .290 |
| Adequate control to ensure privacy | .404 | .085 | .569 | -.157 | .011 | -.096 | .299 |
| Companies will act with high business standards | .536 | .271 | .363 | -.026 | .056 | .116 | -.024 |
| Companies have skills and expertise | .749 | .326 | .127 | .018 | -.187 | .078 | -.151 |
| Companies are dependable | .116 | .205 | .669 | -.025 | .212 | .054 | -.015 |
| Do not have ill intension about consumers | .056 | .660 | .111 | -.089 | -.093 | .049 | .226 |
| Companies are trustworthy | .002 | .485 | .459 | .201 | -.070 | .389 | .121 |
| Credit card info over We is unsafe | -.175 | .041 | .166 | .619 | .121 | .345 | -.124 |
| Risky to give info | .034 | .040 | -.242 | .780 | -.063 | .063 | .013 |
| Uncertainty for providing info | .251 | -.073 | -.074 | .652 | .171 | .004 | -.129 |
| Providing info not matte for low prices | .383 | .099 | -.122 | .019 | .381 | -.082 | .514 |
| Providing info not matte for higher quality | -.017 | .008 | .095 | -.097 | .013 | .047 | .873 |
| Trust to open account w a bank | .318 | .166 | -.070 | .059 | .792 | .042 | .039 |
| Trust to open account w a credit card company | -.012 | .050 | .168 | .056 | .861 | .045 | .060 |
| Confidence for complex and advanved method | .043 | -.067 | .251 | .353 | .478 | .548 | -.069 |
| Confidence for all necessary guaranties | .339 | -.048 | -.070 | .185 | .214 | .690 | -.096 |

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 11 iterations.

## Study II

**Communalities**

| | Initial | Extraction |
|---|---|---|
| Feel safe providing info over Web | 1.000 | .678 |
| Accessible only by intended recipient | 1.000 | .609 |
| Info is not altered in transit | 1.000 | .636 |
| Not hesitate to purchase for security issues | 1.000 | .523 |
| Adequate control to ensure security | 1.000 | .484 |
| Info would not be misused | 1.000 | .431 |
| Control over how info will be used | 1.000 | .610 |
| Later verify info | 1.000 | .535 |
| Companies will not reveal info | 1.000 | .645 |
| Effective mechanism to address violation | 1.000 | .709 |
| Adequate control to ensure privacy | 1.000 | .621 |
| Companies will act with high business standards | 1.000 | .586 |
| Companies have skills and expertise | 1.000 | .499 |
| Companies are dependable | 1.000 | .682 |
| Do not have ill intension about consumers | 1.000 | .839 |
| Companies are trustworthy | 1.000 | .817 |
| Credit card info over Web is unsafe | 1.000 | .410 |
| Risky to give info | 1.000 | .542 |
| Uncertainty for providing info | 1.000 | .671 |
| Providing info not matter for low prices | 1.000 | .635 |
| Providing info not matter for higher quality | 1.000 | .694 |
| Trust to open account with a bank | 1.000 | .780 |
| Trust to open account with a credit card company | 1.000 | .590 |
| Confidence for complex and advanved method | 1.000 | .557 |
| Confidence for all necessary guaranties | 1.000 | .577 |

Extraction Method: Principal Component Analysis.

**Total Variance Explained**

| Component | Initial Eigenvalues | | | Extraction Sums of Squared Loadings | | | Rotation Sums of Squared Loadings | | |
|---|---|---|---|---|---|---|---|---|---|
| | Total | % of Variance | Cumulative % | Total | % of Variance | Cumulative % | Total | % of Variance | Cumulative % |
| 1 | 6.326 | 25.304 | 25.304 | 6.326 | 25.304 | 25.304 | 2.775 | 11.102 | 11.102 |
| 2 | 1.907 | 7.630 | 32.934 | 1.907 | 7.630 | 32.934 | 2.769 | 11.076 | 22.178 |
| 3 | 1.880 | 7.521 | 40.455 | 1.880 | 7.521 | 40.455 | 2.464 | 9.855 | 32.033 |
| 4 | 1.578 | 6.312 | 46.766 | 1.578 | 6.312 | 46.766 | 2.446 | 9.783 | 41.816 |
| 5 | 1.448 | 5.791 | 52.557 | 1.448 | 5.791 | 52.557 | 2.136 | 8.543 | 50.360 |
| 6 | 1.189 | 4.756 | 57.313 | 1.189 | 4.756 | 57.313 | 1.512 | 6.047 | 56.407 |
| 7 | 1.034 | 4.136 | 61.449 | 1.034 | 4.136 | 61.449 | 1.261 | 5.042 | 61.449 |
| 8 | .997 | 3.989 | 65.438 | | | | | | |
| 9 | .876 | 3.506 | 68.944 | | | | | | |
| 10 | .847 | 3.387 | 72.331 | | | | | | |
| 11 | .834 | 3.336 | 75.667 | | | | | | |
| 12 | .712 | 2.848 | 78.515 | | | | | | |
| 13 | .652 | 2.608 | 81.123 | | | | | | |
| 14 | .608 | 2.432 | 83.555 | | | | | | |
| 15 | .561 | 2.246 | 85.801 | | | | | | |
| 16 | .506 | 2.024 | 87.825 | | | | | | |
| 17 | .474 | 1.895 | 89.720 | | | | | | |
| 18 | .452 | 1.810 | 91.530 | | | | | | |
| 19 | .408 | 1.633 | 93.163 | | | | | | |
| 20 | .374 | 1.495 | 94.658 | | | | | | |
| 21 | .342 | 1.367 | 96.025 | | | | | | |
| 22 | .309 | 1.235 | 97.260 | | | | | | |
| 23 | .286 | 1.143 | 98.403 | | | | | | |
| 24 | .251 | 1.005 | 99.408 | | | | | | |
| 25 | .148 | .592 | 100.000 | | | | | | |

Extraction Method: Principal Component Analysis.

**Component Transformation Matrix**

| Component | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| 1 | .510 | .468 | .396 | .429 | .394 | .158 | -.003 |
| 2 | .389 | -.767 | .067 | .432 | -.048 | -.203 | .160 |
| 3 | -.501 | .012 | .764 | .193 | -.281 | -.153 | .155 |
| 4 | -.114 | .311 | -.419 | .668 | -.481 | -.119 | -.153 |
| 5 | .158 | -.044 | .031 | -.038 | -.457 | .792 | .365 |
| 6 | .066 | .256 | -.183 | -.071 | .029 | -.377 | .865 |
| 7 | .543 | .168 | .211 | -.374 | -.567 | -.355 | -.212 |

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

**Component Matrix[a]**

| | Component | | | | | | |
|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Feel safe providing info over Web | .526 | .273 | .268 | .381 | -.049 | -.143 | -.295 |
| Accessible only by intended recipient | .546 | .301 | .064 | .456 | -.018 | .092 | .006 |
| Info is not altered in transit | .476 | .349 | .170 | .481 | -.098 | -.039 | -.126 |
| Not hesitate to purchase for security issues | .451 | .276 | -.384 | .117 | .286 | .019 | .002 |
| Adequate control to ensure security | .534 | .228 | -.138 | .256 | .146 | .083 | .184 |
| Info would not be misused | .569 | -.240 | -.102 | .049 | -.054 | .054 | -.176 |
| Control over how info wil be used | .477 | -.573 | -.030 | .199 | .022 | .028 | -.116 |
| Later verify info | .312 | -.300 | -.267 | .057 | .182 | -.400 | -.283 |
| Companies will not revea info | .516 | -.558 | .093 | .207 | -.036 | .116 | -.025 |
| Effective mechanism to address violation | .640 | -.473 | -.023 | .155 | -.035 | .182 | .132 |
| Adequate control to ensure privacy | .467 | -.404 | .016 | .130 | -.036 | .244 | .402 |
| Companies will act with high business standards | .715 | .238 | -.089 | .027 | .029 | -.070 | -.060 |
| Companies have skills and expertise | .564 | .204 | -.261 | -.059 | .019 | .103 | .240 |
| Companies are dependable | .703 | .040 | .352 | -.137 | -.006 | -.153 | .145 |
| Do not have ill intension about consumers | .536 | .041 | .678 | -.278 | -.022 | -.090 | .075 |
| Companies are trustworthy | .510 | .045 | .651 | -.325 | .064 | -.129 | .070 |
| Credit card info over We is unsafe | -.388 | .055 | .036 | .433 | .245 | -.069 | .052 |
| Risky to give info | -.440 | .033 | .207 | .242 | .435 | -.037 | .235 |
| Uncertainty for providing info | -.601 | .076 | .260 | .300 | .234 | -.039 | .302 |
| Providing info not matter for low prices | .692 | .227 | -.168 | -.165 | .073 | .024 | .208 |
| Providing info not matter for higher quality | .456 | .219 | -.517 | -.298 | -.089 | -.096 | .253 |
| Trust to open account wi a bank | -.114 | .083 | .140 | -.108 | .346 | .775 | -.096 |
| Trust to open account wi a credit card company | .384 | .230 | .050 | -.276 | .219 | .325 | -.397 |
| Confidence for complex and advanved method | .111 | -.160 | -.060 | -.119 | .665 | -.088 | -.226 |
| Confidence for all necessary guaranties | .244 | -.139 | -.039 | -.160 | .599 | -.294 | .160 |

Extraction Method: Principal Component Analysis.

a. 7 components extracted.

**Rotated Component Matrix[a]**

| | Component | | | | | | |
|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Feel safe providing info over Web | .020 | .074 | .235 | .772 | .120 | .061 | -.054 |
| Accessible only by intended recipient | .318 | .192 | .078 | .673 | -.029 | -.090 | .059 |
| Info is not altered in transit | .152 | .080 | .118 | .763 | .006 | -.097 | -.036 |
| Not hesitate to purchase for security issues | .564 | .024 | -.140 | .304 | .084 | .279 | .086 |
| Adequate control to ensure security | .530 | .198 | .043 | .392 | -.054 | .048 | .061 |
| Info would not be misused | .142 | .451 | .063 | .217 | .367 | .147 | .001 |
| Control over how info wi be used | -.044 | .711 | .015 | .124 | .184 | .221 | -.071 |
| Later verify info | .019 | .233 | -.105 | .117 | .251 | .540 | -.318 |
| Companies will not reve info | -.035 | .763 | .124 | .139 | .138 | .093 | -.015 |
| Effective mechanism to address violation | .215 | .780 | .133 | .108 | .152 | .039 | .012 |
| Adequate control to ensure privacy | .288 | .700 | .155 | -.050 | -.068 | -.125 | .030 |
| Companies will act with high business standards | .466 | .129 | .221 | .436 | .301 | .146 | -.019 |
| Companies have skills and expertise | .645 | .151 | .094 | .143 | .172 | -.014 | .045 |
| Companies are dependable | .281 | .245 | .666 | .252 | .158 | .067 | -.085 |
| Do not have ill intension about consumers | .013 | .132 | .881 | .172 | .117 | -.005 | .051 |
| Companies are trustworthy | .028 | .087 | .879 | .128 | .099 | .085 | .053 |
| Credit card info over We is unsafe | -.182 | -.108 | -.273 | .129 | -.518 | .072 | -.032 |
| Risky to give info | -.149 | -.142 | -.045 | -.075 | -.683 | .139 | .079 |
| Uncertainty for providing info | -.243 | -.212 | -.081 | -.094 | -.737 | -.093 | -.004 |
| Providing info not matter for low prices | .671 | .134 | .272 | .170 | .237 | .083 | .037 |
| Providing info not matter for higher quality | .728 | -.032 | -.007 | -.093 | .352 | .018 | -.170 |
| Trust to open account wi a bank | -.030 | .018 | -.039 | -.090 | -.117 | -.028 | .869 |
| Trust to open account wi a credit card company | .132 | -.075 | .184 | .207 | .394 | .231 | .531 |
| Confidence for complex and advanved method | .015 | .047 | .026 | -.048 | -.053 | .714 | .198 |
| Confidence for all necessary guaranties | .270 | .096 | .231 | -.131 | -.183 | .621 | -.074 |

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 9 iterations.

# Appendix F

## Correlation Analysis

## Study I

**Correlations**

| | | SECURITY | PRIVACY | VENDORS | RISK | ECONOMIC | INSTITUT | CONS_TRU |
|---|---|---|---|---|---|---|---|---|
| SECURITY | Pearson Correlation | 1 | .424** | .513** | -.074 | .144 | .239* | -.067 |
| | Sig. (2-tailed) | . | .000 | .000 | .502 | .190 | .028 | .545 |
| | N | 85 | 85 | 85 | 85 | 85 | 85 | 85 |
| PRIVACY | Pearson Correlation | .424** | 1 | .449** | -.071 | .134 | .121 | .002 |
| | Sig. (2-tailed) | .000 | . | .000 | .518 | .222 | .271 | .986 |
| | N | 85 | 85 | 85 | 85 | 85 | 85 | 85 |
| VENDORS | Pearson Correlation | .513** | .449** | 1 | .055 | .269* | .357** | .218* |
| | Sig. (2-tailed) | .000 | .000 | . | .615 | .013 | .001 | .045 |
| | N | 85 | 85 | 85 | 85 | 85 | 85 | 85 |
| RISK | Pearson Correlation | -.074 | -.071 | .055 | 1 | -.077 | .148 | .388** |
| | Sig. (2-tailed) | .502 | .518 | .615 | . | .484 | .176 | .000 |
| | N | 85 | 85 | 85 | 85 | 85 | 85 | 85 |
| ECONOMIC | Pearson Correlation | .144 | .134 | .269* | -.077 | 1 | .245* | .045 |
| | Sig. (2-tailed) | .190 | .222 | .013 | .484 | . | .024 | .685 |
| | N | 85 | 85 | 85 | 85 | 85 | 85 | 85 |
| INSTITUT | Pearson Correlation | .239* | .121 | .357** | .148 | .245* | 1 | .381** |
| | Sig. (2-tailed) | .028 | .271 | .001 | .176 | .024 | . | .000 |
| | N | 85 | 85 | 85 | 85 | 85 | 85 | 85 |
| CONS_TRU | Pearson Correlation | -.067 | .002 | .218* | .388** | .045 | .381** | 1 |
| | Sig. (2-tailed) | .545 | .986 | .045 | .000 | .685 | .000 | . |
| | N | 85 | 85 | 85 | 85 | 85 | 85 | 85 |

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

## Study II

**Correlations**

| | | SECURITY | PRIVACY | VENDORS | RISK | ECONOMIC | INSTITUT | CONS_TRU |
|---|---|---|---|---|---|---|---|---|
| SECURITY | Pearson Correlation | 1 | .280** | .382** | -.235** | .276** | .071 | .015 |
| | Sig. (2-tailed) | . | .000 | .000 | .003 | .000 | .366 | .852 |
| | N | 163 | 163 | 163 | 163 | 163 | 163 | 163 |
| PRIVACY | Pearson Correlation | .280** | 1 | .356** | -.360** | .263** | .030 | .156* |
| | Sig. (2-tailed) | .000 | . | .000 | .000 | .001 | .708 | .047 |
| | N | 163 | 163 | 163 | 163 | 163 | 163 | 163 |
| VENDORS | Pearson Correlation | .382** | .356** | 1 | -.325** | .321** | .150 | .140 |
| | Sig. (2-tailed) | .000 | .000 | . | .000 | .000 | .056 | .075 |
| | N | 163 | 163 | 163 | 163 | 163 | 163 | 163 |
| RISK | Pearson Correlation | -.235** | -.360** | -.325** | 1 | -.467** | -.107 | -.054 |
| | Sig. (2-tailed) | .003 | .000 | .000 | . | .000 | .173 | .495 |
| | N | 163 | 163 | 163 | 163 | 163 | 163 | 163 |
| ECONOMIC | Pearson Correlation | .276** | .263** | .321** | -.467** | 1 | .098 | .143 |
| | Sig. (2-tailed) | .000 | .001 | .000 | .000 | . | .212 | .069 |
| | N | 163 | 163 | 163 | 163 | 163 | 163 | 163 |
| INSTITUT | Pearson Correlation | .071 | .030 | .150 | -.107 | .098 | 1 | .099 |
| | Sig. (2-tailed) | .366 | .708 | .056 | .173 | .212 | . | .211 |
| | N | 163 | 163 | 163 | 163 | 163 | 163 | 163 |
| CONS_TRU | Pearson Correlation | .015 | .156* | .140 | -.054 | .143 | .099 | 1 |
| | Sig. (2-tailed) | .852 | .047 | .075 | .495 | .069 | .211 | . |
| | N | 163 | 163 | 163 | 163 | 163 | 163 | 163 |

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Appendix G

Regression Analysis

## Study I

**Variables Entered/Removed[b]**

| Model | Variables Entered | Variables Removed | Method |
|---|---|---|---|
| 1 | RISK, VENDORS, PRIVACY, SECURITY[a] | . | Enter |

a. All requested variables entered.

b. Dependent Variable: CONS_TRU

**Model Summary**

| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate |
|---|---|---|---|---|
| 1 | .466[a] | .217 | .178 | .75362 |

a. Predictors: (Constant), RISK, VENDORS, PRIVACY, SECURITY

**ANOVA[b]**

| Model | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| 1 | Regression | 12.612 | 4 | 3.153 | 5.552 | .001[a] |
| | Residual | 45.435 | 80 | .568 | | |
| | Total | 58.047 | 84 | | | |

a. Predictors: (Constant), RISK, VENDORS, PRIVACY, SECURITY

b. Dependent Variable: CONS_TRU

**Coefficients[a]**

| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
|---|---|---|---|---|---|---|
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | 1.995 | .648 | | 3.077 | .003 |
| | SECURITY | -.241 | .157 | -.184 | -1.540 | .127 |
| | PRIVACY | -.046 | .161 | -.033 | -.284 | .777 |
| | VENDORS | .394 | .156 | .307 | 2.527 | .013 |
| | RISK | .404 | .114 | .355 | 3.550 | .001 |

a. Dependent Variable: CONS_TRU

**Variables Entered/Removed[b]**

| Model | Variables Entered | Variables Removed | Method |
|---|---|---|---|
| 1 | INSTITUT, ECONOMIC[a] | . | Enter |

a. All requested variables entered.

b. Dependent Variable: RISK

**Model Summary**

| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate |
|---|---|---|---|---|
| 1 | .189[a] | .036 | .012 | .72763 |

a. Predictors: (Constant), INSTITUT, ECONOMIC

**ANOVA[b]**

| Model | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| 1 | Regression | 1.604 | 2 | .802 | 1.515 | .226[a] |
| | Residual | 43.414 | 82 | .529 | | |
| | Total | 45.018 | 84 | | | |

a. Predictors: (Constant), INSTITUT, ECONOMIC

b. Dependent Variable: RISK

**Coefficients[a]**

| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
|---|---|---|---|---|---|---|
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | 3.306 | .445 | | 7.432 | .000 |
| | ECONOMIC | -.129 | .119 | -.121 | -1.078 | .284 |
| | INSTITUT | .160 | .101 | .178 | 1.589 | .116 |

a. Dependent Variable: RISK

## Study II

**Variables Entered/Removed[b]**

| Model | Variables Entered | Variables Removed | Method |
|---|---|---|---|
| 1 | SECURITY[a] | . | Enter |

a. All requested variables entered.

b. Dependent Variable: CONS_TRU

**Model Summary**

| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate |
|---|---|---|---|---|
| 1 | .015[a] | .000 | -.006 | .37333 |

a. Predictors: (Constant), SECURITY

**ANOVA[b]**

| Model | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| 1 | Regression | .005 | 1 | .005 | .035 | .852[a] |
| | Residual | 22.440 | 161 | .139 | | |
| | Total | 22.445 | 162 | | | |

a. Predictors: (Constant), SECURITY

b. Dependent Variable: CONS_TRU

**Coefficients[a]**

| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
|---|---|---|---|---|---|---|
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | 3.965 | .286 | | 13.872 | .000 |
| | SECURITY | .014 | .078 | .015 | .186 | .852 |

a. Dependent Variable: CONS_TRU

**Variables Entered/Removed[b]**

| Model | Variables Entered | Variables Removed | Method |
|---|---|---|---|
| 1 | PRIVACY[a] | . | Enter |

a. All requested variables entered.

b. Dependent Variable: CONS_TRU

**Model Summary**

| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate |
|---|---|---|---|---|
| 1 | .156[a] | .024 | .018 | .36880 |

a. Predictors: (Constant), PRIVACY

**ANOVA[b]**

| Model | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| 1 | Regression | .547 | 1 | .547 | 4.020 | .047[a] |
| | Residual | 21.898 | 161 | .136 | | |
| | Total | 22.445 | 162 | | | |

a. Predictors: (Constant), PRIVACY

b. Dependent Variable: CONS_TRU

**Coefficients[a]**

| Model | | Unstandardized Coefficients | | Standardized Coefficients | | |
|---|---|---|---|---|---|---|
| | | B | Std. Error | Beta | t | Sig. |
| 1 | (Constant) | 3.471 | .275 | | 12.644 | .000 |
| | PRIVACY | .155 | .077 | .156 | 2.005 | .047 |

a. Dependent Variable: CONS_TRU

**Variables Entered/Removed[b]**

| Model | Variables Entered | Variables Removed | Method |
|---|---|---|---|
| 1 | VENDORS[a] | . | Enter |

a. All requested variables entered.

b. Dependent Variable: CONS_TRU

**Model Summary**

| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate |
|---|---|---|---|---|
| 1 | .140[a] | .020 | .013 | .36971 |

a. Predictors: (Constant), VENDORS

**ANOVA[b]**

| Model | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| 1 | Regression | .439 | 1 | .439 | 3.210 | .075[a] |
| | Residual | 22.006 | 161 | .137 | | |
| | Total | 22.445 | 162 | | | |

a. Predictors: (Constant), VENDORS

b. Dependent Variable: CONS_TRU

**Coefficients[a]**

| Model | | Unstandardized Coefficients | | Standardized Coefficients | | |
|---|---|---|---|---|---|---|
| | | B | Std. Error | Beta | t | Sig. |
| 1 | (Constant) | 3.565 | .255 | | 13.983 | .000 |
| | VENDORS | .140 | .078 | .140 | 1.792 | .075 |

a. Dependent Variable: CONS_TRU

**Variables Entered/Removed[b]**

| Model | Variables Entered | Variables Removed | Method |
|---|---|---|---|
| 1 | RISK[a] | . | Enter |

a. All requested variables entered.

b. Dependent Variable: CONS_TRU

**Model Summary**

| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate |
|---|---|---|---|---|
| 1 | .054[a] | .003 | -.003 | .37283 |

a. Predictors: (Constant), RISK

**ANOVA[b]**

| Model | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| 1 | Regression | .065 | 1 | .065 | .468 | .495[a] |
| | Residual | 22.380 | 161 | .139 | | |
| | Total | 22.445 | 162 | | | |

a. Predictors: (Constant), RISK

b. Dependent Variable: CONS_TRU

**Coefficients[a]**

| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
|---|---|---|---|---|---|---|
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | 4.259 | .353 | | 12.053 | .000 |
| | RISK | -.062 | .090 | -.054 | -.684 | .495 |

a. Dependent Variable: CONS_TRU

**Variables Entered/Removed[b]**

| Model | Variables Entered | Variables Removed | Method |
|---|---|---|---|
| 1 | RISK, SECURITY, PRIVACY, VENDORS[a] | . | Enter |

a. All requested variables entered.

b. Dependent Variable: CONS_TRU

**Model Summary**

| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate |
|---|---|---|---|---|
| 1 | .191[a] | .037 | .012 | .36993 |

a. Predictors: (Constant), RISK, SECURITY, PRIVACY, VENDORS

**ANOVA[b]**

| Model | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| 1 | Regression | .822 | 4 | .206 | 1.502 | .204[a] |
| | Residual | 21.622 | 158 | .137 | | |
| | Total | 22.445 | 162 | | | |

a. Predictors: (Constant), RISK, SECURITY, PRIVACY, VENDORS

b. Dependent Variable: CONS_TRU

**Coefficients[a]**

| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
|---|---|---|---|---|---|---|
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | 3.285 | .658 | | 4.993 | .000 |
| | SECURITY | -.065 | .085 | -.066 | -.768 | .444 |
| | PRIVACY | .137 | .087 | .138 | 1.575 | .117 |
| | VENDORS | .123 | .090 | .122 | 1.365 | .174 |
| | RISK | .023 | .099 | .020 | .234 | .816 |

a. Dependent Variable: CONS_TRU

**Variables Entered/Removed [b]**

| Model | Variables Entered | Variables Removed | Method |
|---|---|---|---|
| 1 | INSTITUT, ECONOMIC[a] | . | Enter |

a. All requested variables entered.

b. Dependent Variable: RISK

**Model Summary**

| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate |
|---|---|---|---|---|
| 1 | .471[a] | .222 | .212 | .28868 |

a. Predictors: (Constant), INSTITUT, ECONOMIC

**ANOVA[b]**

| Model | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| 1 | Regression | 3.805 | 2 | 1.902 | 22.827 | .000[a] |
| | Residual | 13.334 | 160 | .083 | | |
| | Total | 17.138 | 162 | | | |

a. Predictors: (Constant), INSTITUT, ECONOMIC

b. Dependent Variable: RISK

**Coefficients[a]**

| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
|---|---|---|---|---|---|---|
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | 5.437 | .295 | | 18.418 | .000 |
| | ECONOMIC | -.362 | .055 | -.461 | -6.579 | .000 |
| | INSTITUT | -.052 | .059 | -.062 | -.885 | .378 |

a. Dependent Variable: RISK

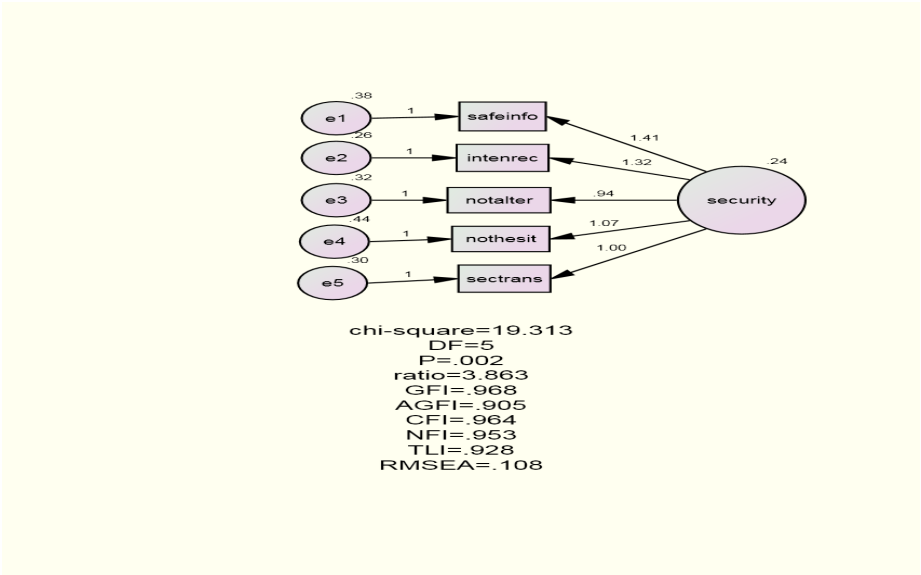
Appendix H

Structural Equation Modeling

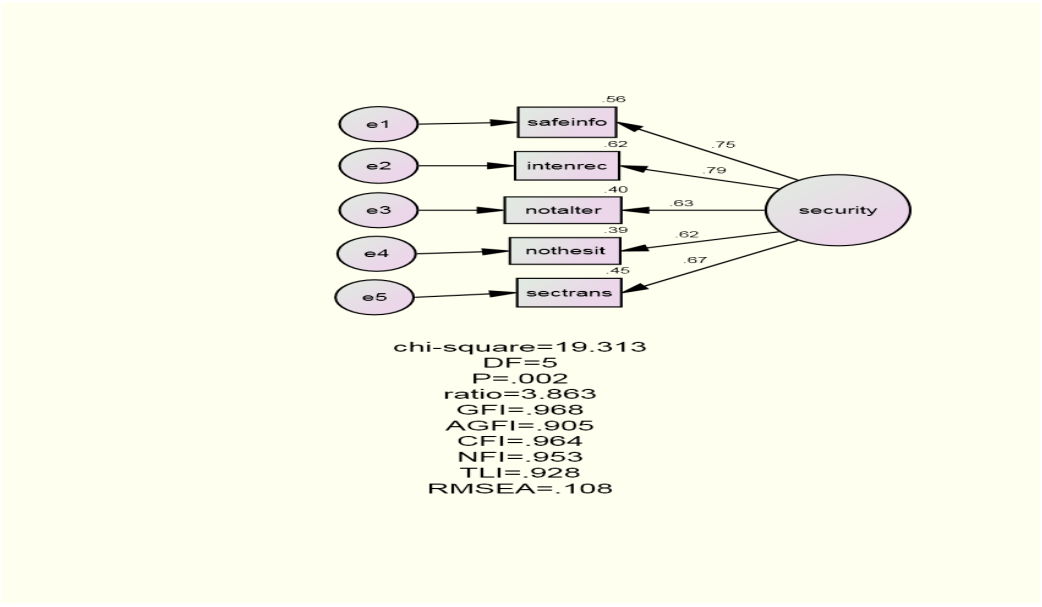
Confirmatory Factor Analysis

Perceived Information Security

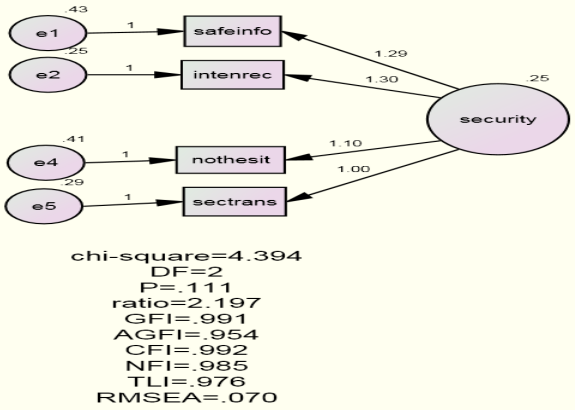
**Unstandardized estimates**



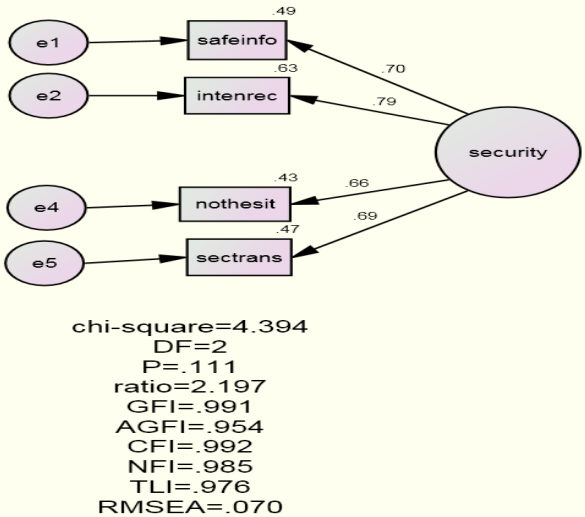

**Standardized estimates**



**Unstandardized estimates**

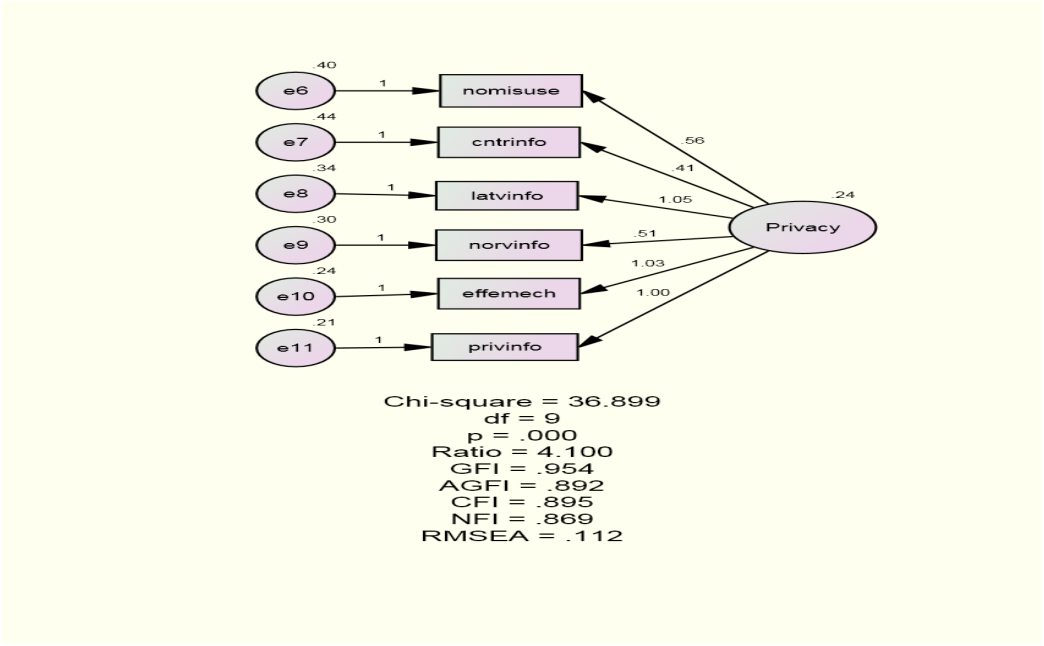



**Standardized estimates**

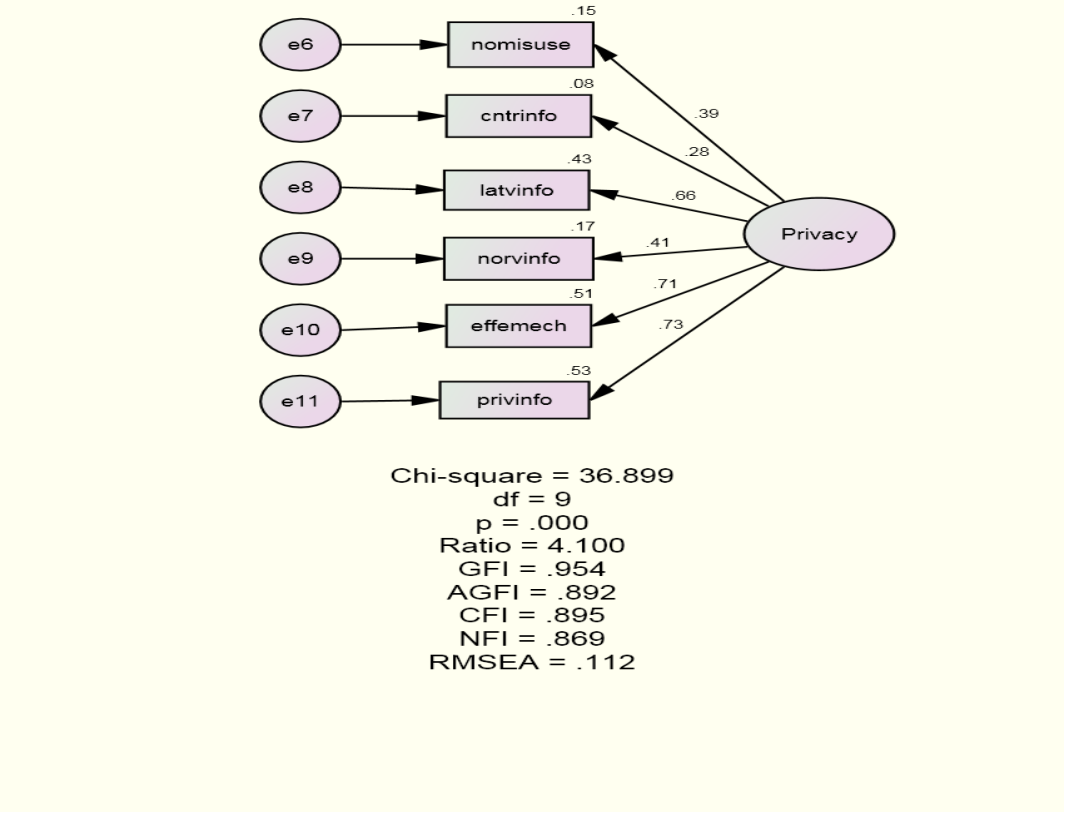


Perceived Information Privacy

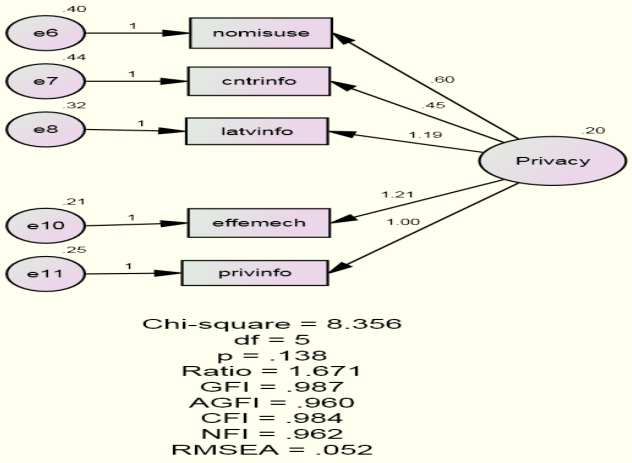
**Unstandardized estimates**



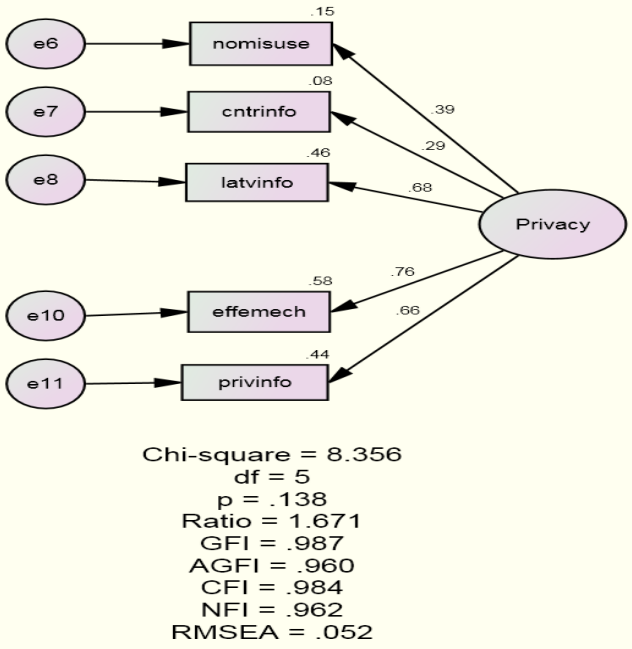

**Standardized estimates**



**Unstandardized estimates**

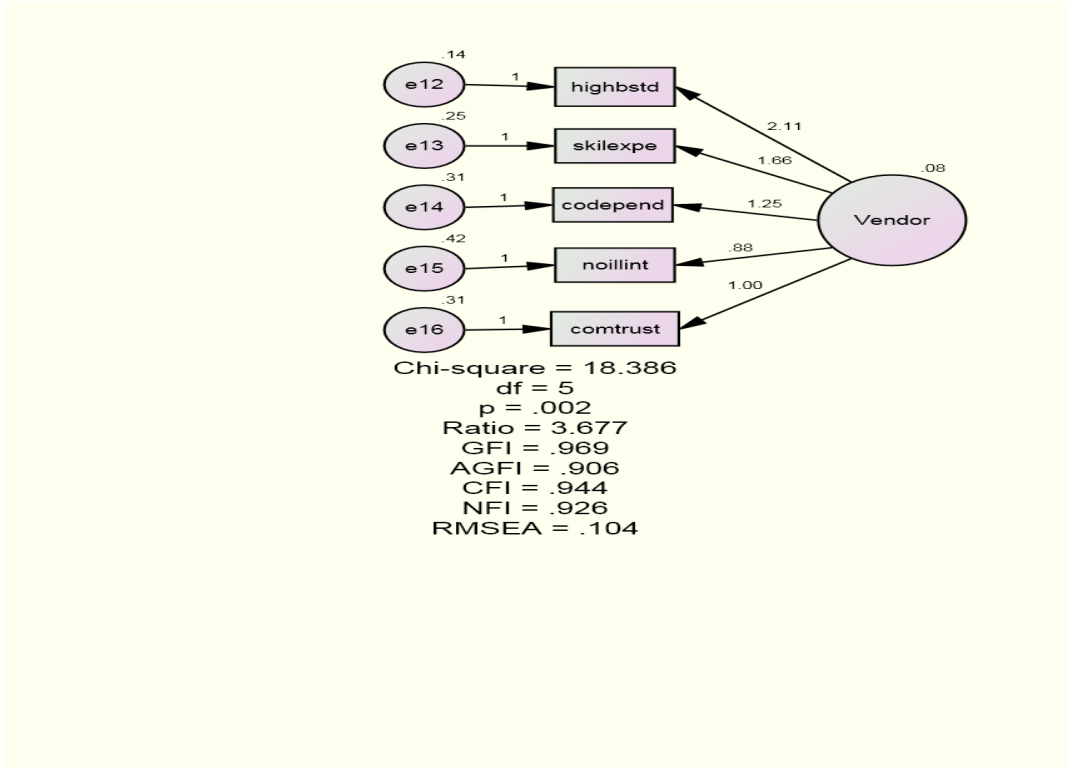



**Standardized estimates**

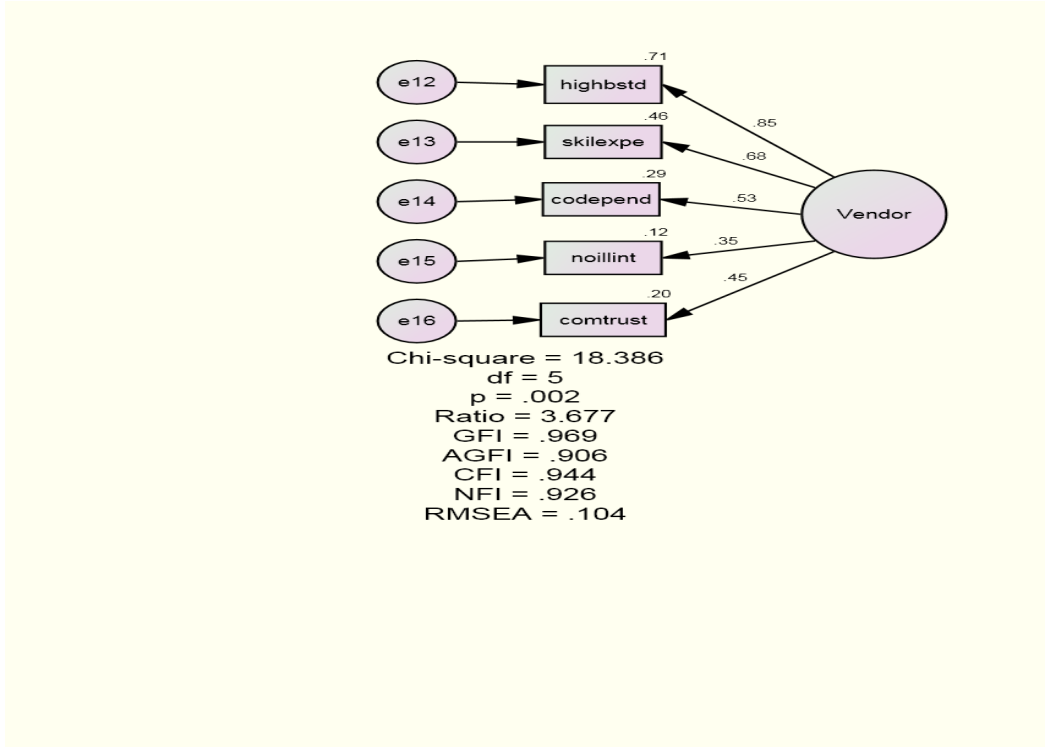


Trustworthiness of Web Vendors

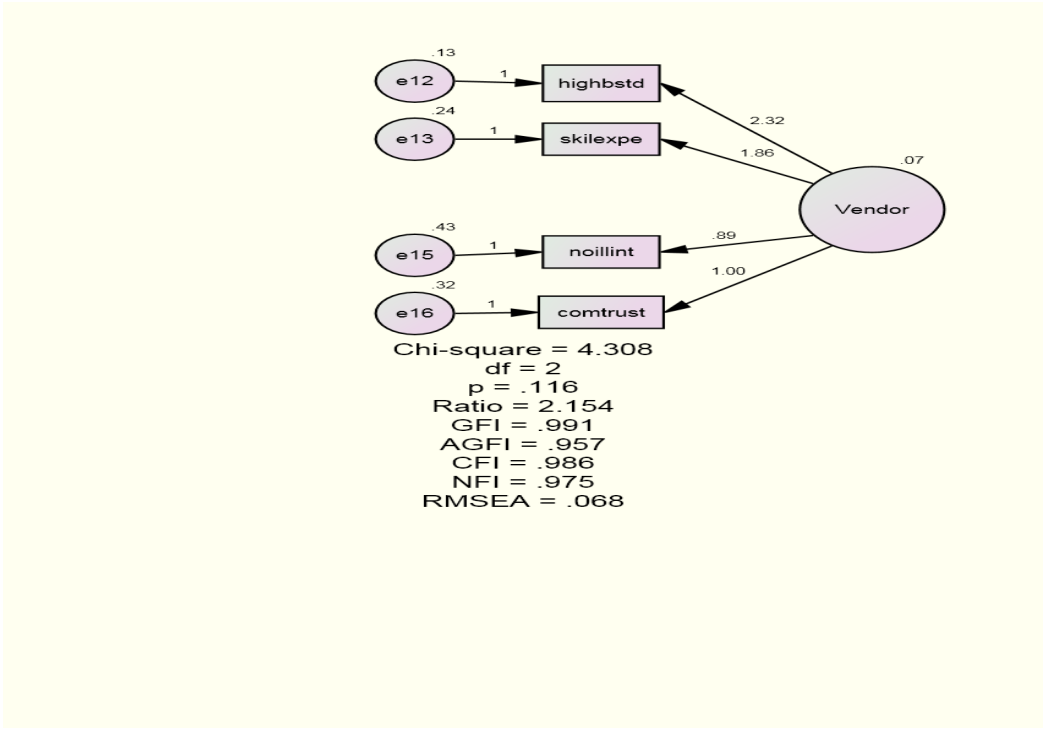
**Unstandardized estimates**



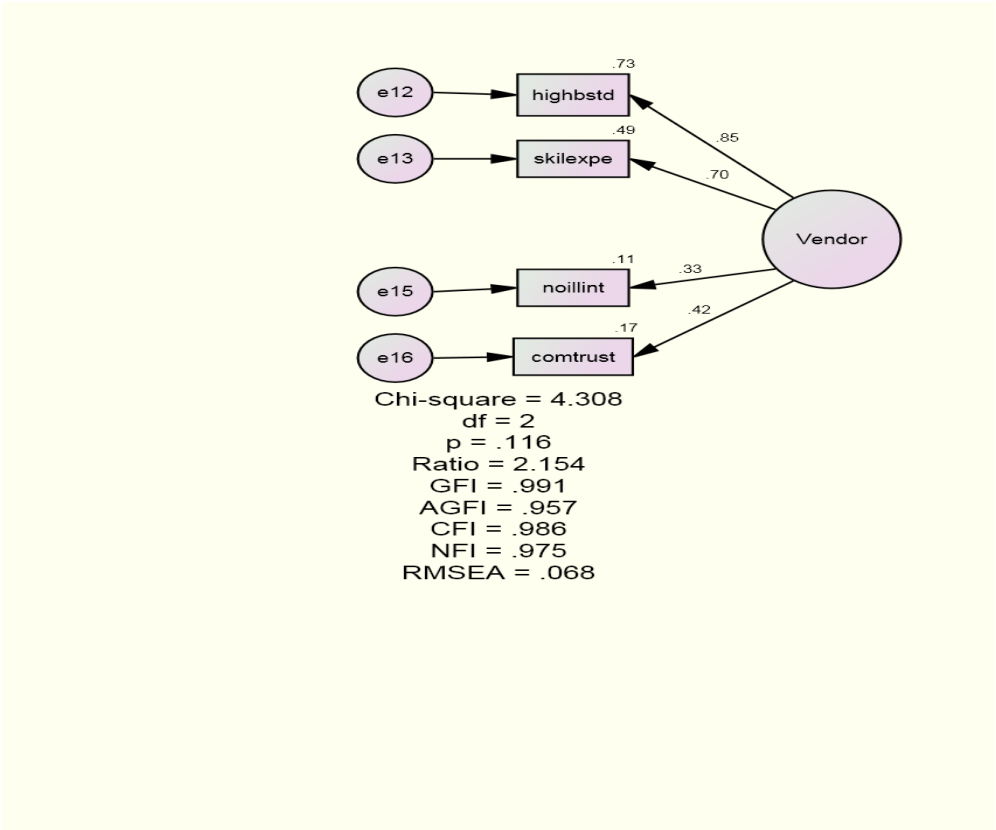

**Standardized estimates**



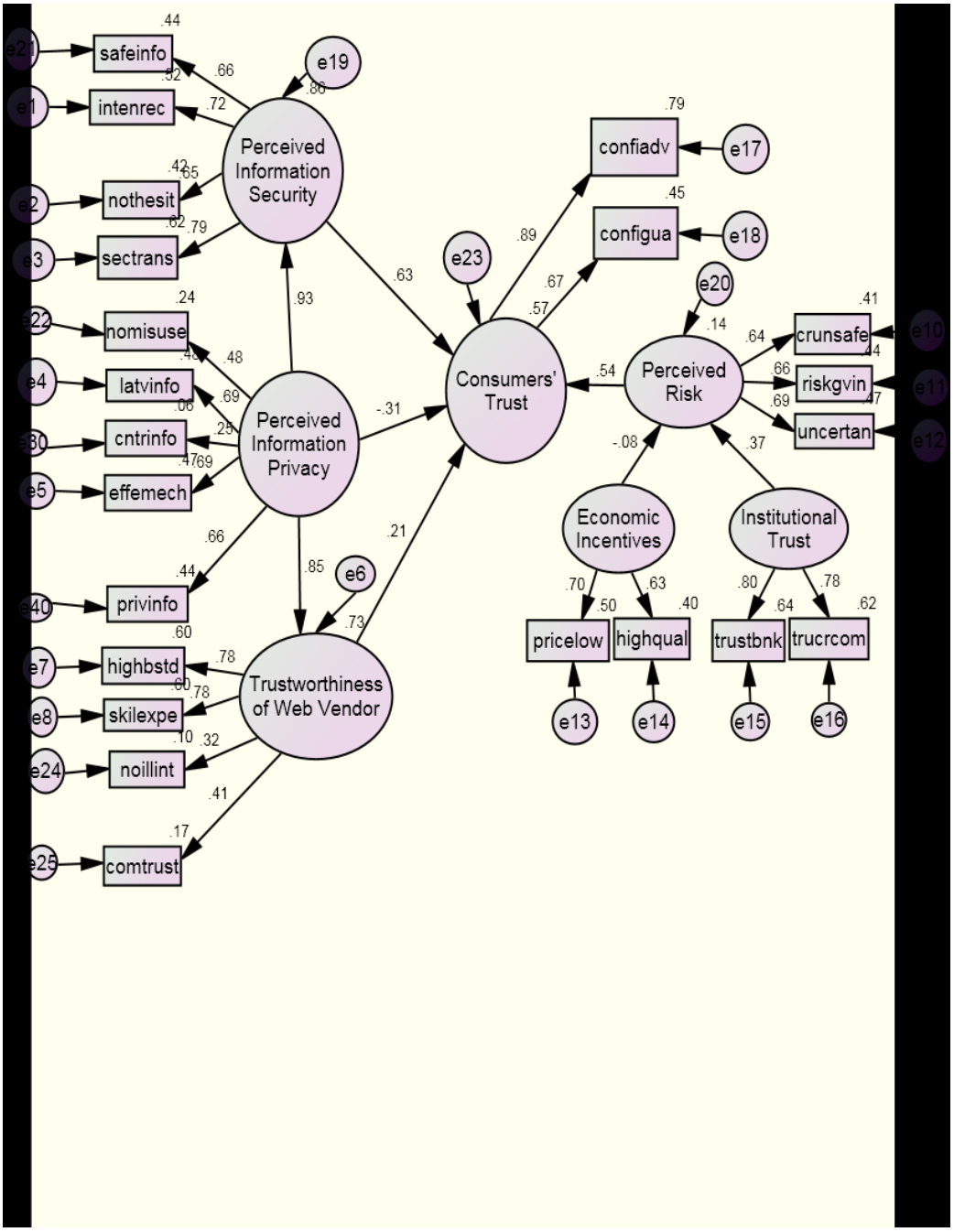
**Unstandardized estimates**



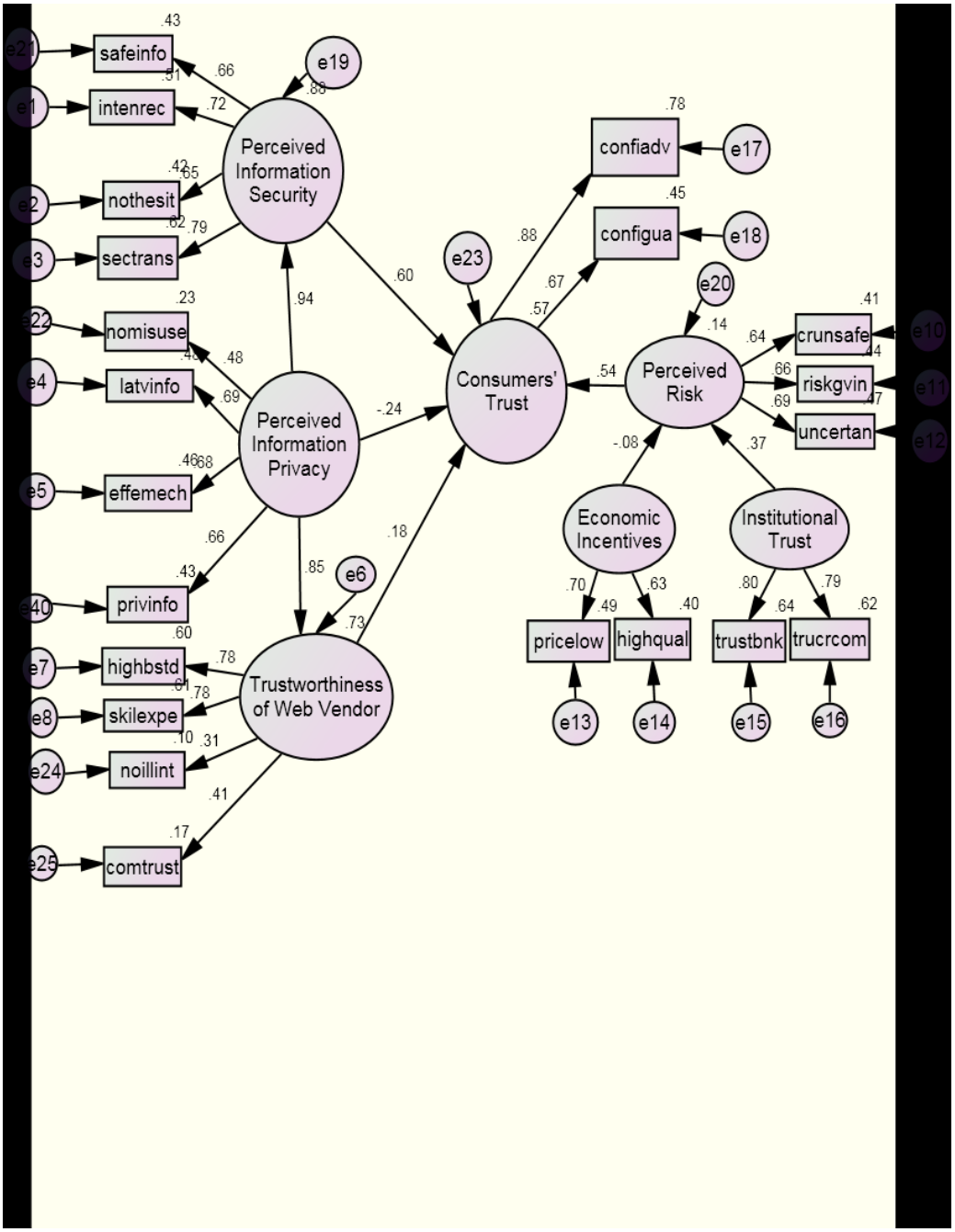

**Standardized estimates**



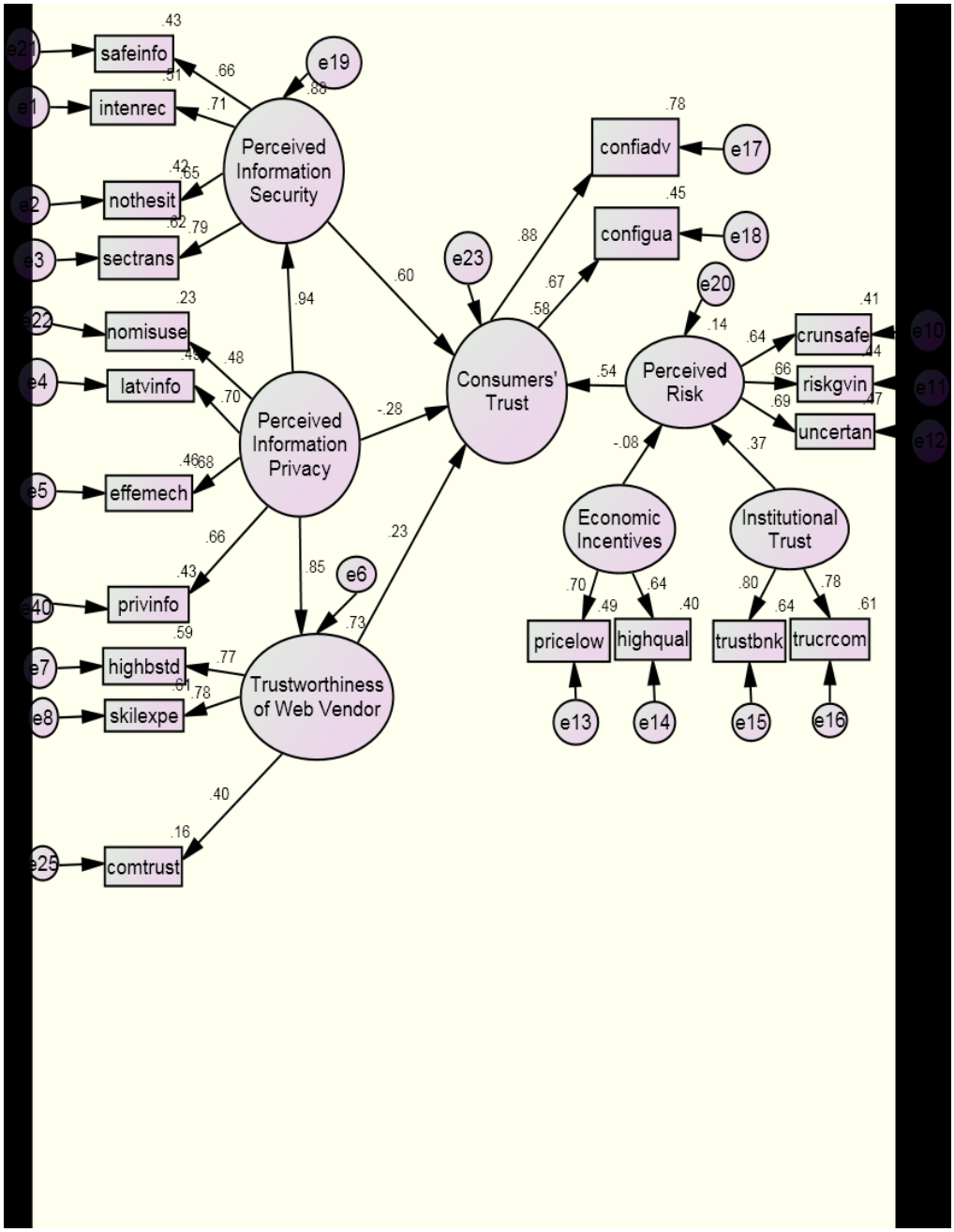
**AfterCFA_ Test**
**Standardized estimates**



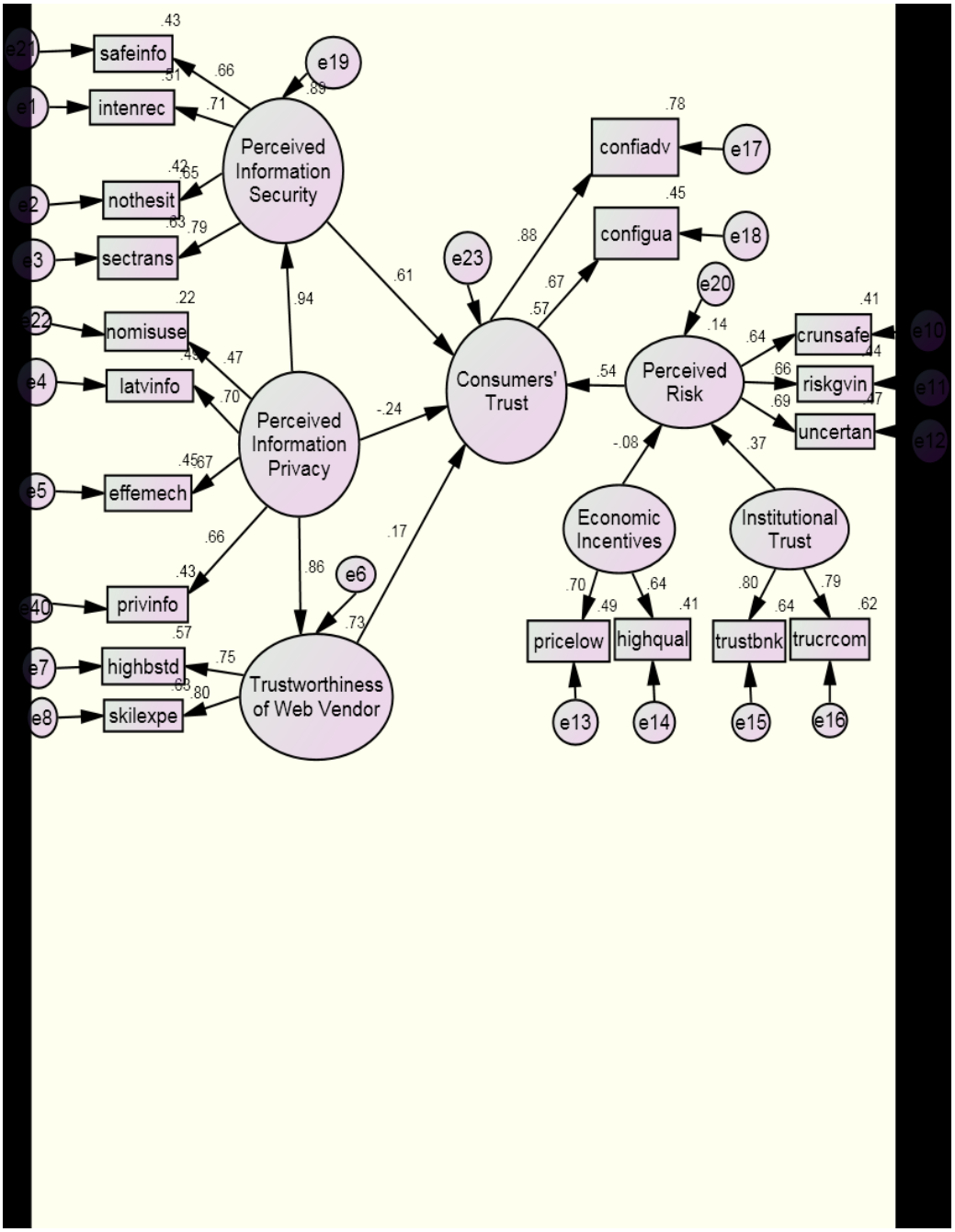
**Test_2_Remove(Privacy_cntrinfo)**
**Standardized estimates**



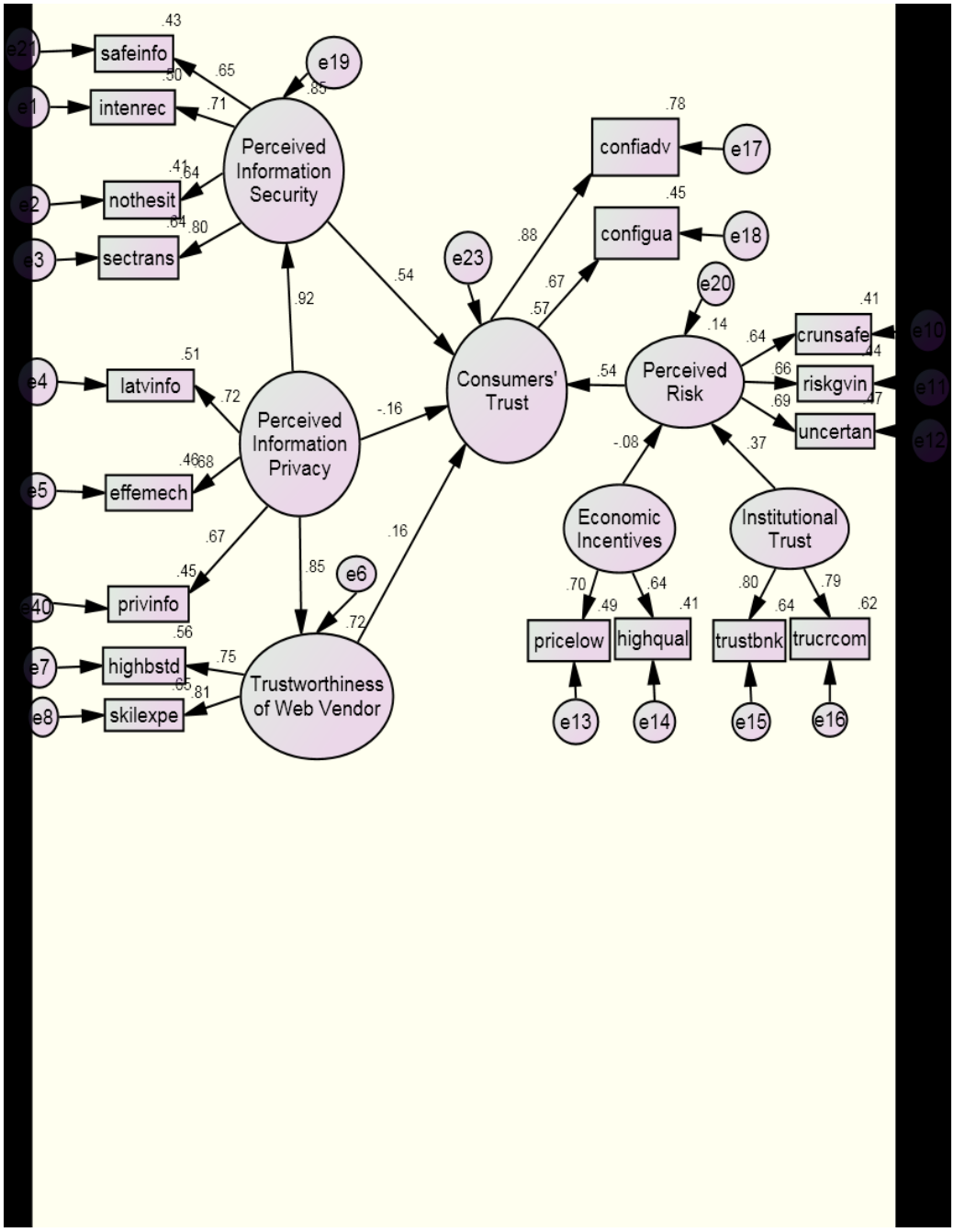
**Test_3_Remove(Vendor_noillint)**
**Standardized estimates**



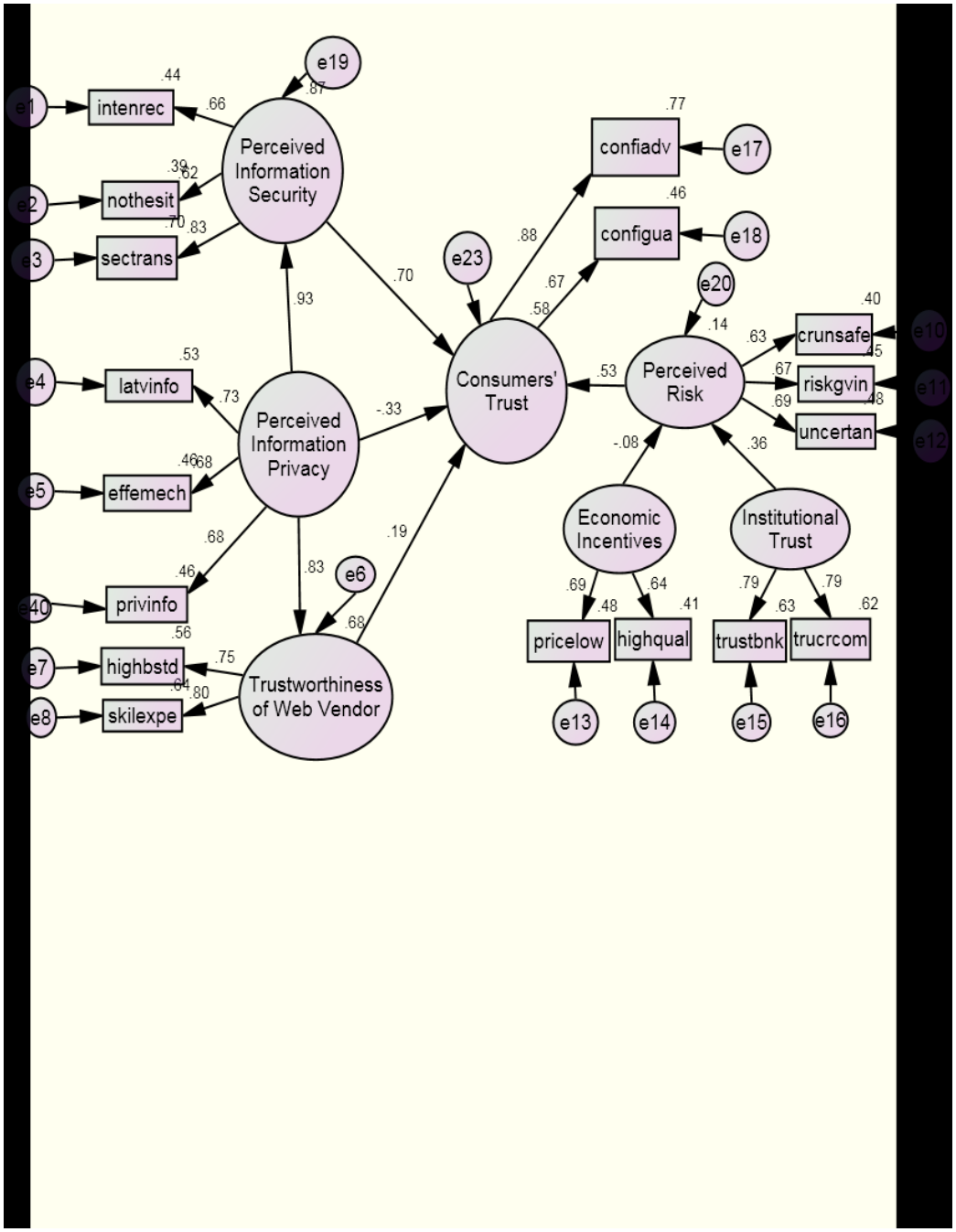
**Test_4_Remove(Vendor_comtrust)**
**Standardized estimates**



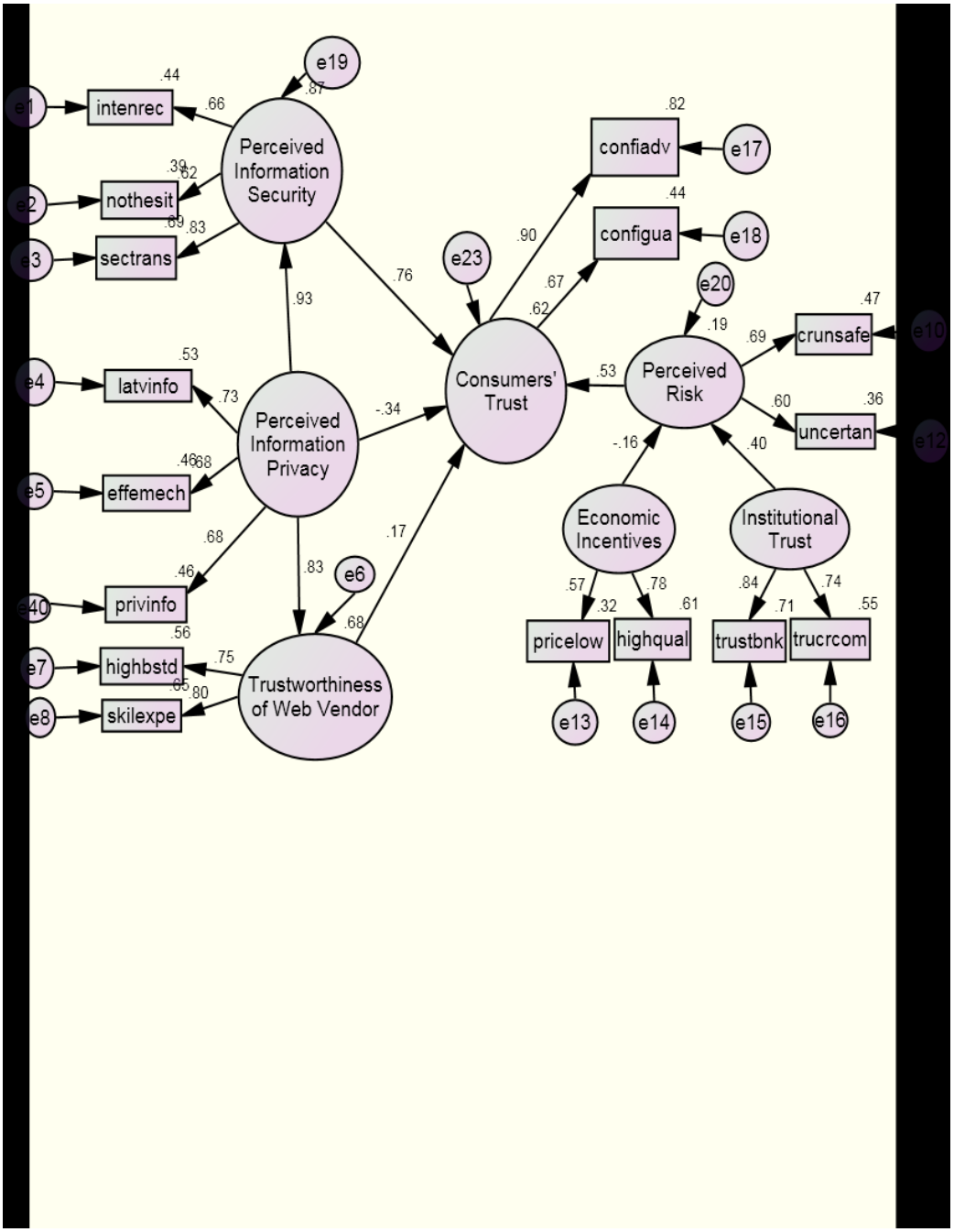
**Test_5_Remove(Privacy_nomisuse)**
**Standardized estimates**



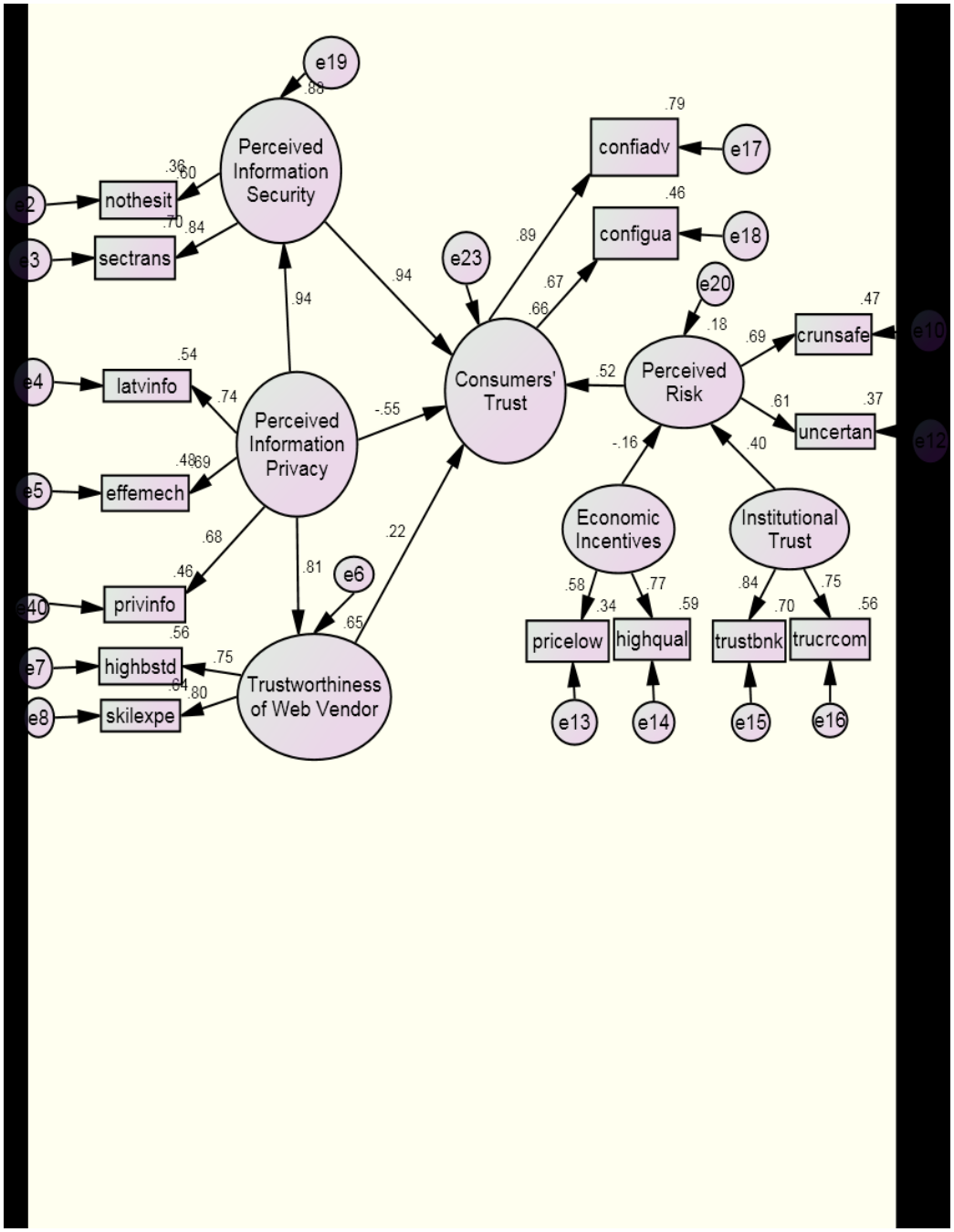
**Test_6_Remove(Security_safeinfo)**
**Standardized estimates**



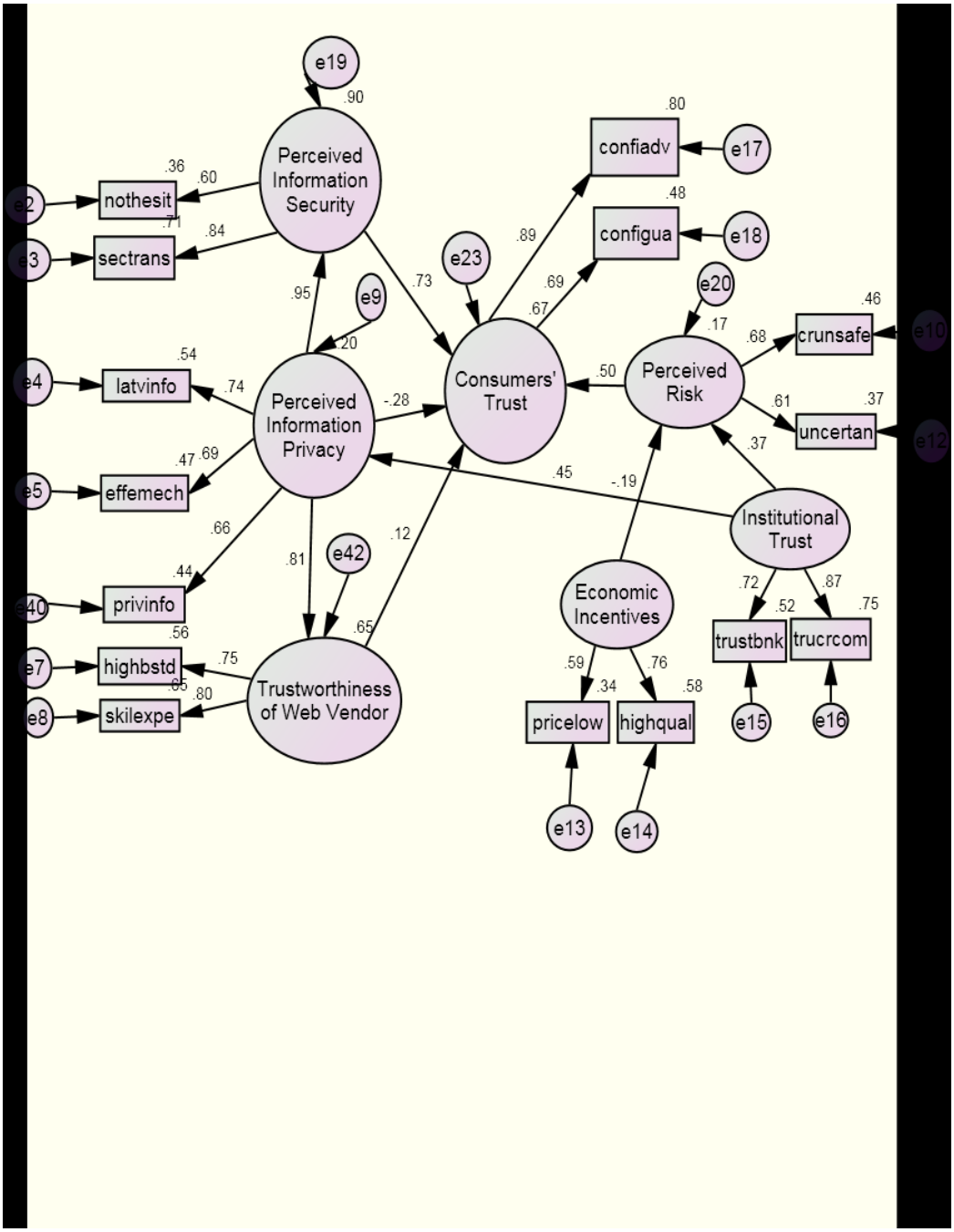
**Test_7_Remove(Risk_riskgvin)**
**Standardized estimates**



**Test_8_Remove(Security_intenrec)**
**Standardized estimates**



**Test_9_Institute→Privacy**
**Standardized estimates**



**Test 10_Economic→Privacy**
**Standardized estimates**