IJCSS, Vol.1, No.1, 2009
ISSN: 1803-8336

Security in Electronic Transaction on the Internet (An Empirical Study)

Khalid S. Husain
King Abdulaziz University
P.O. Box 18388
Jeddah, 21415
966-2-6952401
Khusain@kau.edu.sa

Wajdi H. Aljedaibi
King Abdulaziz University
P.O. Box 9031
Jeddah, 21413
966-2-6952401
Waljedaibi@kau.edu.sa

ABSTRACT

Electronic commerce enables companies to be more efficient and flexible in their internal operations to work more closely with their suppliers, and to be more responsive to the needs and expectations of their customers. There are several factors that prevent the widespread use of E-commerce such as lack of knowledge and lack of trust in internet security. In this research effort we conduct an empirical study that aims to show what is the effect of the Internet security on doing online transactions. The leading reason for not making transactions on the Internet was found to be related to Internet security and to the fear of being robbed by hackers or Internet Pirates. We conclude by drafting a range of recommendation to more effective e-commerce activities on the internet.

1. INTRODUCTION

Using the Internet is becoming an everyday event in our lifes, whether to send an e-mail, look for information or just to have fun. Yet, there is a very important application that people can use on the Internet which is the ability to shop and make electronic transactions. Although the Internet is drawing much more attention over the years, the number of people who are really making electronic transactions is not that big. Lack of security in the Internet is the accused to be the leading reason for people not to do more transactions. The purpose of this paper is to indicate the effect of Internet security on doing transactions over the Internet. This paper provides an empirical study to find out what the real inhibitor is.

1.1 What is Electronic Commerce?

Electronic commerce can be defined as "any form of business transaction in which the parties interact electronically rather than by physical exchanges or direct physical contact."[1] Electronic commerce enables companies to be more efficient and flexible in their Internal operations to work more closely with their suppliers, and to be more responsive to the needs and expectations of their customers. It allows companies to select the best suppliers regardless of their geographical location and to sell to global market.

One case of electronic commerce which is a special case of electronic trading (a supplier provides goods or services to a customer in return for payment) is electronic retailing, where the customer is an ordinary consumer rather than another company. In this study we will focus on electronic retailing and what factors preventing people from making transactions on the Internet. Electronic commerce can be sub-divided into four distinct categories:[2]

- Business - Business
- Business - Consumer
- Business - Administration
- Consumer - Administration

Where business - consumer is the focus of our study. This category has greatly expand with the advance of the World Wide Web. There are now shopping malls all over the Internet offering all manner of consumer goods, from cakes to motor cars.

1.2 Why Electronic Commerce?

The impact of electronic commerce will be widespread, both on companies and on society. Individual members of society will be presented with new ways of purchasing goods, accessing information and services. Choice will be greatly extended, and restrictions of geography and time eliminated. "The overall impact on lifestyle could well be comparable to, say, that of the growth in car ownership or the spread of the telephone."[3] Electronic commerce includes electronic trading of physical goods and

[1] Electronic Commerce - An Introduction, http://www.ispo.cec.be/ecommerce/introduc.htm#WHAT
2 Electronic Commerce - An Introduction, http://www.ispo.cec.be/ecommerce/introduc.htm#CATEGORIES
3 Electronic Commerce - An Introduction, http://www.ispo.cec.be/ecommerce/introduc.htm#IMPACT

IJCSS, Vol.1, No.1, 2009
ISSN: 1803-8336

services of electronic material. As Dr. Dan Ryan says "Electronic commerce is going to make us rich, because the money moves faster, and the faster the money moves the faster we get rich." Electronic commerce offers several opportunities to suppliers and benefits to customers:[4]

Supplier Opportunity	Customer Benefit
* Global presence	* Global choice
* Cost savings	* Quality of service
* Shorten or eradicate supply chains	* Personalized products & services
* Mass customization	* Rapid response to needs
* Novel business competitiveness	* Substantial price reductions
* Improved competitiveness	* New products and services

The Internet is rapidly becoming the information superhighway of a global electronic marketplace. The population of the Internet is growing rapidly, in 2007 the number of Web users was 6 billion worldwide. The following graph gives us some statistics about the Internet which reflects how big the market growing.

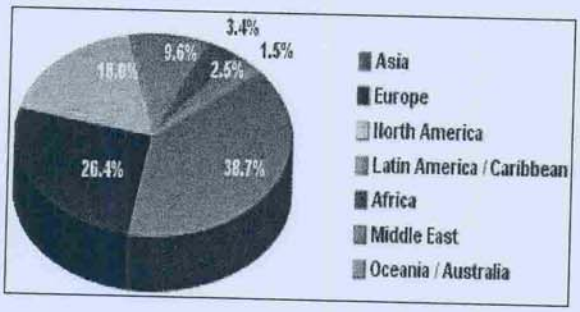

Figure -1- World Internet Users (2007)
(Source: www.internetworldstats.com)

The following table gives the Internet usage statistics and population statistics.

WORLD INTERNET USAGE AND POPULATION STATISTICS

World Regions	Population (2007 Est.)	Population % of World	Internet Usage, Latest Data	% Population (Penetration)	Usage % of World	Usage Growth 2000-2007
Africa	941,249,130	14.2 %	44,361,940	4.7 %	3.4 %	882.7 %
Asia	3,733,783,474	56.5 %	510,478,743	13.7 %	38.7 %	346.6 %
Europe	801,821,187	12.1 %	348,125,847	43.4 %	26.4 %	231.2 %
Middle East	192,755,045	2.9 %	33,510,500	17.4 %	2.5 %	920.2 %
North America	334,659,631	5.1 %	238,015,529	71.1 %	18.0 %	128.2 %
Latin America/Caribbean	569,133,474	8.6 %	126,203,714	22.2 %	9.6 %	598.5 %
Oceania / Australia	33,569,718	0.5 %	19,175,836	57.1 %	1.5 %	151.6 %
WORLD TOTAL	6,606,971,659	100.0 %	1,319,872,109	20.0 %	100.0 %	265.6 %

Figure -2- World Internet Users and Population Stats (2007)
(Source: www.internetworldstats.com)

[4]Electronic Commerce - An Introduction,
http://www.ispo.cec.be/ecommerce/introduc.htm#SUPPLIER

Today the Internet continues to grow day by day making Global Village a reality. The following table graph shows the incredibly fast evolution of the Internet from 1995 till the present time and the prediction for 2010.

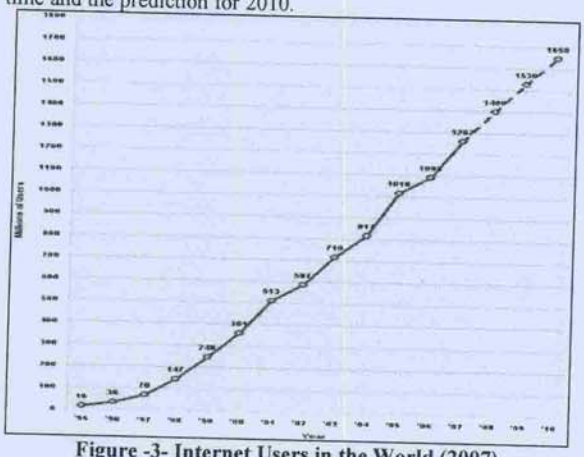

Figure -3- Internet Users in the World (2007)
(Source: www.internetworldstats.com)

The following table gives the Internet usage in the Middle East.

INTERNET USERS IN THE MIDDLE EAST AND IN THE WORLD

MIDDLE EAST REGION	Population (2007 Est.)	Pop. % of World	Internet Users, Latest Data	% Population (Penetration)	Usage % of World	Use Growth (2000-2007)
Total in Middle East	192,755,045	2.9 %	33,510,500	17.4 %	2.5 %	920.2 %
Rest of the World	6,414,216,614	97.1 %	1,286,361,609	20.1 %	97.5 %	259.6 %
WORLD TOTAL	6,606,971,659	100.0 %	1,319,872,109	20.0 %	100.0 %	265.6 %

Figure -4- Internet Usage in the Middle East (Source: www.internetworldstats.com)

The following graph shows the Internet penetration in the Middle East by December 2007.

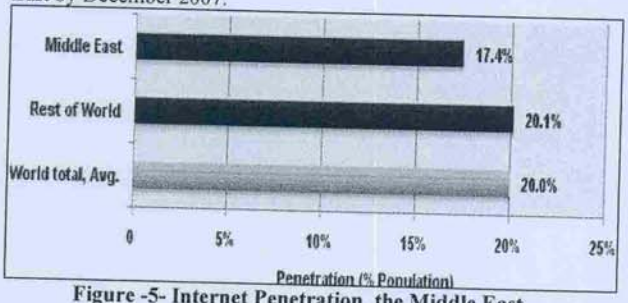

Figure -5- Internet Penetration the Middle East
(Source: www.internetworldstats.com)

Internet Usage

The figure below shows the online activities of USA broadband users, 2007 (% of total time spent online)

IJCSS, Vol.1, No.1, 2009
ISSN: 1803-8336

Figure -9- The Online Activities of USA Broadband Users, 2007 (% of total time spent online)
Source: Media-Screen, "Netpp|Play" as provided to eMarketer May 7, 2007.

eCommerce World Wide

eMarketer projects that US retail e-commerce spending will reach $131.3 billion in 2007.This figure roughly matches Cowen and Co.'s forecast of $129 billion. In addition, eMarketer expects USA retail e-commerce spending to reach $243.5 billion in 2011.

eMarketer estimates that in 2006, 65.6% of US Internet users purchased a product online.The Pew Internet & American Life Project came up with a somewhat higher figure of 71%.

The graph below shows that USA Internet shoppers spent an average of $972 in 2006. eMarketer expects this figure to grow by roughly 13% each year, to a value of $1,829 in 2011.

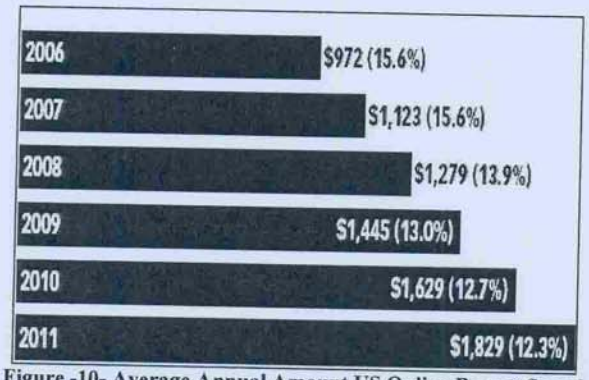

Figure -10- Average Annual Amount US Online Buyers Spend Online, 2006-2011 (% increase vs. prior year)
Ages 14+; excludes travel (May 2007)
Source: eMarketer, May 2007.

The Graph below shows the Reasons that Online vs. Offline Shopping Is More Convenient or Better according to US Online Shoppers, June-July 2007 (% of respondents)

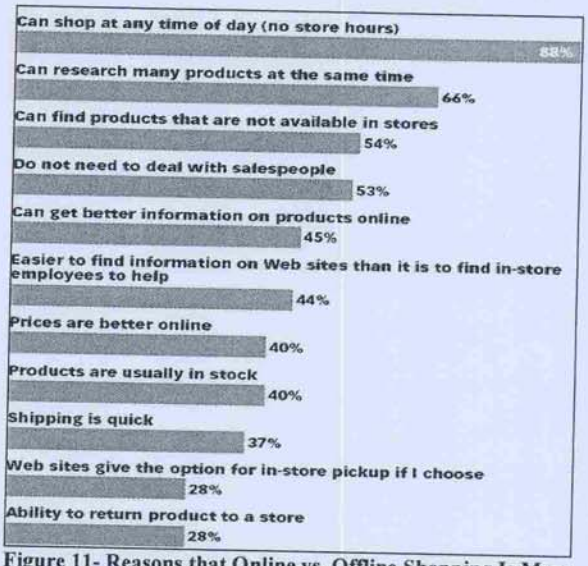

Figure 11- Reasons that Online vs. Offline Shopping Is More Convenient or Better according to US Online Shoppers, June-July 2007 (% of respondents) August 2007.
Source: Sterling Commerce and Deloitte, "What Consumers Want in their Shopping Experience" August 2007.

In 2006, B2C e-commerce sales for the five major markets in the Asia-Pacific region totaled only $59.1 billion, and Japan accounted for a tiger's share of the sales. But things are changing. eMarketer forecasts that B2C e-commerce sales in the region will grow at a 23.3% annual rate, reaching $168.7 billion in 2011. "Japan was the largest market in the region, by far, with a 62.3% share of online sales in 2006," says Jeffrey Grau, eMarketer Senior Analyst and author of the new report, Asia-Pacific B2C E-Commerce: Focus on China and India. "But by 2011, Japan and South Korea, the region's other mature market, will both lose share to two up-andcoming online markets—China and India." Both China and India are growing rapidly, but they are far from reaching their vast potential. "A number of hurdles, common to both countries, must be cleared to ensure sustainable long-term growth," says Grau. "Immature online payment systems, poor delivery networks and distrust between buyers and sellers, to name just a few."

eCommerce in Saudi Arabia

Saudi Arabia's Internet users spend over $3.28bn in B2C e-commerce during 2007. Based on the survey findings, the Arab Advisors Group estimates e-commerce users in Saudi Arabia to exceed 3.5 million consumers representing 14.26% of the population. A new major survey of the Internet users in Saudi Arabia, was concluded by the Arab Advisors Group. The survey report, Saudi Arabia Internet users and e-commerce Survey 2008 was released on Jan 6, 2008 and provides the results of a major comprehensive online survey of Internet users in Saudi Arabia. The survey covered the Internet usage, e commerce and cellular usage and habits of the Internet users in Saudi Arabia. The survey field work was conducted between November and December 2007. The survey report includes online replies from 1,919 respondents. Quality control checks and personal validation were conducted by Arab Advisors Group's team. The survey was conducted on the general Internet population, including both

IJCSS, Vol.1, No.1, 2009
ISSN: 1803-8336

genders and all age groups across Saudi Arabia. The online survey yields a confidence level of 99% with a margin of error of less than 2%. According to the survey results, 46.4% of Internet users in Saudi have Internet access at work, while 36.6% use Internet cafes and 34.3% use WiFi hot spots. A full 23.7% do not access the Internet except from their homes. Naturally, access methods overlapped. While the survey covered Internet users, it also probed the reasons behind why other members of the same households surveyed do not use the Internet. Based on the feedback of Internet users, computer illiteracy, lack of interest, lack of a perceived need to use the Internet and being too young to use the Internet are the main reasons for keeping non-Internet users in Saudi from using the Internet. The survey also revealed that the vast majority of Internet users in Saudi use Hotmail, Yahoo! mail, and Gmail for their personal email service. Regional Arabic-focused email providers have less than a 10% share of the Internet users in Saudi Arabia. There is also plenty of service provider overlap (when users use more than one email service). 42.2% Saudi Arabia's e-commerce users make their payments through credit cards. Another 11.5% reported using Internet shopping cards provided by their banks.

1.3 Retardation to Electronic Commerce

As mentioned earlier, of the 50 million web users 54% were not likely to make on-line purchases in the future. As a leading inhibitor preventing people from actually making transactions online comes the lack of trust in the security of electronic payments. Another inhibiting factor is lack of knowledge. Few of the people using the Internet had heard about the security offered by SSL (A security protocol).

The Internet is generally perceived as not secure enough for transmitting sensitive data such as payments or credit card numbers. Other factors that inhibit people from making transactions on the Internet is lack of products offered, and not being able to see and touch the products. The growth of electronic transactions over the Internet might also be effected by the following factors:

- Gender
- Age
- Education
- Occupation
- Region
- Income

As mentioned earlier, networks or more precisely the Internet security is accused as the leading inhibitor preventing people from actually making transactions online. Other factors that might effect the problem also are as the following:

- Poorly designed web sites
- The reputation of the company offering the product
- The complexity of transactions over the Internet

In the following sections of this paper and after giving a preview about the problem, we will prepare ourselves to conduct an empirical study trying to find out what the real inhibitor is. In doing so several steps will be taken as part of the preparation of the study. Our study will mainly focus on trying to find the reason why 54% of the people will not make transactions through the Internet any more, in doing so we will formulate an hypothesis and conduct an empirical study to test it, data from our study will be further investigated by doing explanatory and statistical analysis that will either assist or refute our hypothesis.

2. STUDY DESIGN

2.1 Hypothesis

As we mentioned in the previous section different factors can effect the decision of making transactions on the Internet, and in order to formulate our hypothesis we will adopt the lack of security on the Internet as the primarily factor inhibiting people from making transactions over the Internet.

The problem can now be stated as follows: "What is the effect of Internet security on doing transactions over the Internet?" Notice that in formulating our hypothesis we should make a relation between two or more variables which in our case are the Internet security and transactions on the Internet. Our hypothesis can now be stated as follows: "Lack of security on the Internet is the leading reason for not making more transactions through the Internet."

In order to test our hypothesis, different issues has to be considered like:

- Variables (Independent, Dependent, Confounding)
- Population and generalization
- Data gathering

After testing our hypothesis, data gathered from experiment will be further investigated and the results collected from the experiment along with the analysis done on it will be presented.

In this study we will measure the number of people who think that the lack of security on the Internet is the leading inhibiting factor that is keeping them from doing more transactions through the Internet, to do so we will pass a survey to see people opinions about the biggest issue that is preventing them from doing transactions through the Internet. The following questionnaire will be used, notice that we are also collecting other related data that we might use in our study.

1- How much money have you spent through Internet transactions overall?
A) None
B) $1 - $50
C) $51 - $500
D) Over $500

2- Do you feel that the current level of security provided by specially designed Internet transaction systems (those that do not use credit card number) is sufficient?
A) Yes
B) No

3- How secure do you feel those Internet transaction systems that do not use credit card numbers are compared to actually giving your credit card number over the Internet?
A) Less secure
B) As secure
C) More secure

4- What is the biggest factor that is keeping you from making more transactions through the Internet?
A) Lack of product offered
B) Web sites too poorly designed to be useful
C) The reputation of the companies offering the products
D) Fear of being robbed by hackers or Internet Pirates
E) Not being able to see and touch the products
F) Afraid of money or merchandise getting lost
G) Concern about revealing too much personal information
H) Transactions are too complicated over the Internet
I) Other

IJCSS, Vol.1, No.1, 2009
ISSN: 1803-8336

2.2 Variables

Different variables can effect transactions on the Internet, of these variables as we mentioned earlier are:

- Gender
- Education
- Age
- Income
- Occupation
- Lack of knowledge
- Internet security

In our study we are concerned with the issue of security on the Internet, and therefore our hypothesis is testing the effect of the Internet security and whether the lack of security is the strongest reason inhibiting people from doing that.

In our study, the dependent variable will be the reason people think that is their biggest worry (Internet security) and we will measure it by counting the number of people who chose this reason. The other independent variables that we have and can effect our results are: gender, education, age, income, occupation, and lack of knowledge. Since all these variables are not considered in our study and their effect is not studied by our hypothesis, they are treated as confounding variables. In order to eliminate the effect of these variables we will rely on randomization to take care of their effect, this might raise a threat to validity to out results later on.

Since we have more than two independent variables, those not chosen in the experiment are confounding variables. They may be found to have some influence over the dependent variable and offer alternative explanations for variations.

2.3 Population

This study will be conducted on will include users of the Internet in general, mostly of the age 20 and over, this is an attempt to control one of the independent variables that we are not testing its effect in our hypothesis, in doing so we are eliminating the threat to validity that might arise from this variable such as the need of authorization for dependent people. The study will also be conducted on college students, graduates, undergraduates, and people with at least college degree; this will eliminate the effect of the independent variable (education level). The study will not differentiate between males and females, we think gender will not significantly effect our results, therefore this variable will not be controlled and we will rely on randomization to take care of its effect in the study. The study will not consider the income and the occupation of the participants, although it might have an effect on our results, we think that it will not effect the issue of security. Finally, the variable (lack of knowledge) which we will not control in this study and again we will rely on randomization to take care of its effect as both knowledgeable people and people who do not know much about the Internet are expected to participate in the study.

In summery, our population will consist of people both males and females of the age 20 years old and older with a college degree or at least working toward one, and they are users of the Internet.

2.4 Data Collection

The procedure we followed to collect the data was to send out questionnaire forms via E-mail and self distributing among students. We were aiming for at least 1,000 participants (which was estimated by a power analysis, section 3.1). Data were collected and grouped according to question number on a spread sheet ready to run both explanatory and statistical analysis.

2.5 Anticipated Results

As the issue of Internet security is accused to be the leading inhibiting factor that is preventing people from doing more transactions through the Internet, we anticipated our data to show a respond that confirms that claim from the participants of the study. The collected data is anticipated to show that by a statistical significance on the number of people who responded with choice (D) to question number four in the questionnaire form among all other choices. This kind of result will assist our hypothesis to a degree that will depend on how significant was that reason among the other reasons. If we counted any significance on any of the other reasons than (D), that will refute our hypothesis.

3. ANALYSIS

After collecting the data we may start exploring it and do our analysis that will refute or assist our hypothesis. A total of 1,120 persons participated in this study, results were collected personally and via E-mail which was very helpful, around 56% of the total sample size participated via E-mail. The response of the participant is shown on the next page :

1) How much money have you spent through Internet transactions overall?

Answer	Count	Percentage
None	460	41%
$1 - $50	156	14%
$51 - $500	336	30%
Over $500	168	15%
Total	1120	100%

Table 3.1

As we can see from the response of this question, 59% of the people have spent money through the Internet transactions. This number is very interesting to us as we are investigating this issue and trying to prove that the lack of Internet security is what's keeping people from making more transactions through the Internet.

2) Do you feel that the current level of security provided by specially designed Internet transaction systems (those that do not use credit card numbers) is sufficient?

Answer	Count	Percentage
Yes	437	39%
No	683	61%
Total	1120	100%

Table 3.2

Notice that the number of people who responded with a yes is very close to the number of people who responded with no, which gives us an indication that the problem is not only a problem of revealing the credit card number, instead it is a problem of security in general where a transaction on the Internet involves the credit card number, revealing personal information, and the ability

IJCSS, Vol.1, No.1, 2009
ISSN: 1803-8336

to trace the transaction which is more general problem and not only transactions over the Internet are sensitive to it. this result will help us focus on the security on the Internet as a general issue as we can see there is a significant number of people who are still concerned about security even if the transaction does not involve credit card numbers. This assumption is clarified by the results gathered from the following question:

3) How secure do you feel those Internet transaction systems that do not use credit card numbers are compared to actually giving you credit card number over the Internet?

Answer	Count	Percentage
Less Secure	347	31%
As Secure	582	52%
More Secure	191	17%
Total	1120	100%

Table 3.3

which confirms our assumption, where more than half of the people think that transactions that do not involve credit card numbers are as secure as those requires credit card numbers. Next is our primarily question in the survey:

4) What is the biggest factor that is keeping you from making more transactions through the Internet?

Answer	Count	Percentage
A) Lack of Products Offered	336	30%
B) Web Sites Too Poorly Designed to be Useful	67	6%
C) The Reputations of the Companies Offerring The Products	34	3%
D) Fear of Being Robbed by Hackers or Inherent Pirates	347	31%
E) Not Being Able to See and Touch the Products	146	13%
F) Afraid of Money or Merchandise Getting Lost	123	11%
G) Concern About Revealing too Much Personal Information	39	3.5%
H) Transactions are Too Complicated Over the Internet	28	2.5%
Total	1,120	100%

Table 3.4

As we can see from table 3.4 and as we anticipated, the leading reason for not making transactions on the Internet is shown to be the one related to Internet security and the fear of being robbed by hackers or Internet Pirates. At this level, the data gathered about our hypothesis is pretty much supporting it; next we will perform a statistical analysis to show the degree of support. As at this level of analysis, we can clearly see that more participants choose the fear of being robbed by hackers or Internet Pirates as the leading factor that is inhibiting them from making more transactions through the Internet.

3.1 Statistical Analysis

In this section we will perform a statistical analysis on the collected data to show the degree of support to our hypothesis. We will use the Chi-test of dependency to show if making transaction on the Internet is dependent on how secure is the Internet. The following is a power analysis that we used to choose our sample size. The first table shows the FAKE data that we anticipate under the corresponding sample size. We proposed three samples 500, 1000, and 1500 people. Under each column is a fake data that we anticipate to be the number of people who will choose the corresponding reason if that was the sample size.

FAKE DATA

Population	500 PPL	1000 PPL	1500PPL	Total
Lack of Products Offered	70	140	210	41%
Fear of Being Robbed by Hacked or Internet Pirates	150	300	450	14%
Not Being Able to See and Touch the Products	110	220	330	30%
Total	330	660	990	100%

Table 3.5

The next table(3.6) is the corresponding expected data under the same proposed samples.

EXPECTED DATA

Population	500 PPL	1000 PPL	1500 PPL	Total
Lack of Products Offered	110	220	330	41%
Fear of Being Robbed by Hacked or Internet Pirates	110	220	330	14%
Not Being Able to See and Touch the Products	110	220	330	30%
Total	330	660	990	100%

Table 3.6

By performing a Chi-test on each of the proposed samples individually, the Chi-test gave us the following result:

CHI-TEST

Population	50 PPL	100 PPL	150 PPL
	0.233506	0.054525	0.012732

As we can see a sample of 1120 participants will sufficient to show statistical significance in the reason associated with our hypothesis in our study. Next we performed a Chi-test on the data we have collected from asking people about their biggest fear from doing more transactions through the Internet.

IJCSS, Vol.1, No.1, 2009
ISSN: 1803-8336

ACTUAL COUNTS

Answer	Count
A) Lack of Products Offered	336
B) Web Sites Too Poorly Designed to be Useful	67
C) The Reputations of the Companies Offerring The Products	34
D) Fear of Being Robbed by Hackers or Inherent Pirates	347
E) Not Being Able to See and Touch the Products	146
F) Afraid of Money or Merchandise Getting Lost	123
G) Concern About Revealing too Much Personal Information	39
H) Transactions are Too Complicated Over the Internet	28
Total	1,120

Table 3.7

The expected counts as follows:

EXPECTED COUNTS

Answer	Count
Lack of Products Offered	124.40
Web Sites Too Poorly Designed to be Useful	124.40
The Reputations of the Companies Offerring The Products	124.40
Fear of Being Robbed by Hackers or Inherent Pirates	124.40
Not Being Able to See and Touch the Products	124.40
Afraid of Money or Merchandise Getting Lost	124.40
Concern About Revealing too Much Personal Information	124.40
Transactions are Too Complicated Over the Internet	124.40
Other	124.40
Total	1119.60

Chi Test	**0.000285**

Table 3.8

As we can see the Chi-test refute the null hypothesis that these reasons are independent. We can then conclude that these reasons are dependent and that Internet transactions are dependent on the given reasons. The P value of (0,000285) is an indicator that if there was no relation between Internet transactions and the given reasons then the numbers listed under the actual counts table will likely appear with a (0,000285) chance.

The following Chi-test was done on the top three reasons found in the study to show if any of them is really significant among the other two reasons.

Actual Counts

Answer	Count
Lack of Products Offered	354
Fear of Being Robbed by Hackers or Inherent Pirates	364
Not Being Able to See and Touch the Products	163
Total	881

Table 3.9

Expected Counts

Answer	Count
Lack of Products Offered	352
Fear of Being Robbed by Hackers or Inherent Pirates	361
Not Being Able to See and Touch the Products	150
Total	863

Chi Test	**0.487644979**

Table 3.10

As we can see the Chi-test fail to support that the reason related to the security of the Internet is significantly better of the other two reasons. As shown before the reason associated with the Internet security was the most chosen reason among the others, clearly there are other reasons that concern people when it comes to making transactions through the Internet and these reasons are some how almost as important to the people as the lack of security in the Internet. So, in conclusion there is an evidence that the lack of security in the Internet is the leading inhibiting factor from making more transactions through the Internet but it is not very strong. The P value of (0,482481) indicates that the numbers listed under the actual counts table above can appear with probability (0,482481), thus the reason related to Internet security is not significantly distinguished from the other two top reasons.

In summery, electronic commerce is the logical extention to any business. If you are selling products over the Internet, it is essential that you have the ability to perform secure transactions for your customer to build some kind of trust between you and them. Offering your customers a secure way of making transactions over the Internet is critical to your success. As we saw from the study consumers are still hesitant to make transactions through the Internet. So, suppliers need to keep in mind that if their customers are not confident in the security, it is likely they will not purchase or make transactions at all. The following sections are going to address the needs of customers and how to achieve those needs.

4. PAYMENT FROM THREE PROSPECTIVES

This section discusses the concerns of the three parties to a payment: the customer, the merchant, and the financial service provider. It identifies the characteristics of a payment mechanism that are important to each party.

- **The Customer :** Customers want to make sure that the money in their accounts is safe and not stolen by some one else. They do not want to invest time learning how to use new payment system. They do not like paying transaction fees. They like instant transactions, and a good technical choice of payment method.[5]
- **The Merchant :** Merchants concern is to sell products and services, but it depends on the payment model used by the customers. Merchants are also concerned with transaction

[5] Andrew B. Whinston & Ravi Kalakota, Readings in Electronic Commerce, (Addison-Wesly Longman, Inc., 1997) 230.

IJCSS, Vol.1, No.1, 2009
ISSN: 1803-8336

fees, the time to complete a transaction, and the risk from counterfeit or stolen payment instruments or customer with insufficient funds to complete payment.[6]

- **The Financial Service Provider :** The financial service providers provide a service for both customers and merchants. They want to make a profit for their services. They want to have more customers to increase their profit. The ideal situation for a financial service provider is to be the only game in town, with all transactions processed by their server or servers.[7]

5. TRANSACTION SECURITY

Transaction security has become very important and necessary because of the increasing number of merchants trying to spur commerce online. Consumer confidence in the reliability and protection of business transactions against third party threats must be reinforced before electronic commerce can succeed.

Unsure of security, consumers are unwilling to provide credit card payment information over the Internet. The following are five "security requirements" that include the security needs of electronic commerce:[8]

- Privacy: The ability to control who sees (or can not see) information and under what terms.
- Authenticity: The ability to know the identities of communicating parties.
- Integrity: The assurance that stored or transmitted information is unaltered.
- Availability: The ability to know when information and communication services will (or will not be) available.
- Blocking: The ability to block unwanted information or instructions.

5.1 Types of Online Transactions

The type of transaction depends on the type of data (or content) being sent across the network. The different categories of data are as the following:[9]

- Public data: This type of data has no security restrictions amd may be read by anyone. Such data should be protected from unauthorized modification.
- Copyright data: This type of data is copyrighted but not secret. The owner of the data is willing to provide it, but wishes to be paid for it. In order to maximize profit security must be tight.
- Confidential data: This type of data contains content that is secret but the existence of the data is not a secret (like bank account, personal files, etc..).
- Secret data: This type of data is a secret and must be kept confidential at all times. It is necessary to monitor and log all access to secret data.

[6]Andrew B. Whinston & Ravi Kalakota, Readings in Electronic Commerce, (Addison-Wesly Longman, Inc., 1997) 230.
[7]Andrew B. Whinston & Ravi Kalakota, Readings in Electronic Commerce, (Addison-Wesly Longman, Inc., 1997) 230.
[8]Andrew B. Whinston & Ravi Kalakota, Electronic Commerce: A Maneger's Guide, (Addison-Wesly Longman, Inc., 1997) 135.
[9]Andrew B. Whinston & Ravi Kalakota, Electronic Commerce: A Manager's Guide, (Addison-Wesly Longman, Inc., 1997) 135.

5.2 Requirements for Transaction Security

There are three basic requirements for transaction security:

5.2.1 Transaction Privacy

In other term called unauthorized network monitoring, or packet sniffing but until now, nothing guarantee the protection of the messages of the Internet users. Their sending and receiving are not interrupted, read, or changed by others. One insecure system on the Internet can break in any remote system not only local machines. Because computer sitting contains all the information that a Sniffer needs to enter other machines, such as log-in ID, password, and user name. Hackers break into a computer and install a packet sniffing program that provide Sniffer attacks to monitor specific net work track, such as Telnet or FTP session. A Sniffer can gather information foe several days on local users entering into remote machines.

5.2.2 Transaction Confidentiality

The electronic commerce environment must ensure that all message traffic is confidential . After successful delivery to their destination gateways, messages must be removed from the public environment, leaving only the accounting record of entry and delivery, including message length, authentication data, and perhaps the audit trail of message transfer agents.[10]

Confidentiality is important for transactions involving sensitive data such as credit card numbers, and will become even more important when data, such as employee records and social security numbers, begin traversing the network.

5.2.3 Transaction Integrity

The contents of electronic commerce transactions between the client and the server must be secret. So no one can add, delete, or change during submission, validation, processing, or delivery. Therefore, ensuring information integrity includes error detection codes or check sums, sequence numbers, and encryption techniques.

6. INTERNET SECURITY

In general, security concerns in electronic commerce can be divided into concerns about user authorization, and concern about data and transaction security. The following are some Internet security terms that need to be in mind:[11]

- Authorization: A way to verify that message senders are who they say they are.
- Integrity: Ensuring that information will not be accidentally or maliciously altered or destroyed.
- Reliability: Ensuring that systems will perform consistently and at an acceptance level of quality.
- Encryption: A process of making information indecipherable except to those with a decoding key.
- Firewall: A filter between a corporate network and the Internet that keeps the corporate network secure from intruders, but allows authenticated corporate users

[10]Andrew B. Whinston & Ravi Kalakota, Electronic Commerce: A Manager's Guide, (Addison-Wesly Longman, Inc., 1997) 137.
[11]Andrew B. Whinston & Ravi Kalakota, Electronic Commerce: A Manager's Guide, (Addison-Wesly Longman, Inc., 1997) 124.

IJCSS, Vol.1, No.1, 2009
ISSN: 1803-8336

uninhibited access to the Internet.

- Spoofing: A way of creating counterfeit packets with private IP (Internet) addresses in order to gain access to private networks and steal information.
- Denial of service: An attack on the information and communications services by a third party that prevents legitimate users from using the infrastructure.

Suppliers or providers should keep some or all of the above security terms in mind to provide a secure transactions for their customers.

7. ENCRYPTION AND TRANSACTION SECURITY

Encryption is transforming the message to a readable form only with a decryption key. Electronic commerce relies heavily on encryption. A "key" is a very large number, a line of zeros and ones to make it impossible to a hacker who obtains the encrypted information as it passes on the network to recover the original message.

There are two main kinds of encryption. the older is called "single-key" or "secret-key" encryption. The more recent one is called "public-key" encryption.

7.1 Secret-Key Encryption

Also known as symmetric encryption, requires the use of shared key between a small group. Both the encrypted who send a purchase order, and the decrypted that can read the scrambled ciphertext use the same secret key. All parties must know and trust each other to protect the copy from the risk of other hearing parties. It is hard to see secret-key encryption becoming a dominant player in electronic commerce, because it can not ensure safe electronic commerce. So, if secret-key encryption can not ensure safe electronic commerce, what can? The solution is a newer form of encryption known as public key encryption.[12]

7.2 Public-key Encryption

Also known as asymmetric encryption, uses two mathematically related keys: a key to encrypt the message and a different key to decrypt the message. Each party uses a pair of keys: one is public for other parties, and another is private for its owner. So friends can share a private e-mail message with their private key. Public-key encryption makes it impossible for a hacker to recover the original message.[13] Another outstanding public-key method used in online commerce today is called Digital Signatures.

7.2.1 Digital Signatures

Digital signature is a secure commerce that provides a way to connect the message with the sender and for sender authentication and privacy, by using public-key encryption. A digital signature is a cryptographic mechanism equivalent of "signing" for purchases.[14]

7.2.2 Digital Certificates

It is an identity proof, the certificate authority creates a message containing the party's name a his or her public key to make sure that the digital signature and the public-key belong to the same party. It provides an easy and convenient way to ensure that the participants in an electronic commerce transaction can trust each other. For example, in the credit card industry, visa provides digital certificate to the card holder.[15]

People often assume that encryption is enough to protect a business from possible danger. However, encryption provides transaction security but does not do much to prevent unauthorized access to computers, information, and the databases. The following section discusses firewalls and network security.

8. FIREWALLS AND NETWORK SECURITY

A firewall is a software or a hardware that let external users with specific characteristic to access a protected network. This system allows insiders to access the services on the outside while allowing access from the outside on special basis. Firewall is installed as an approach to accomplish a security policy between the corporate network and the Internet. Firewalls is also necessary to protect the Internet networks, assets, and client confidentiality from bothering by sponges.

Firewall is located at a gateway point to facilitate a single check point for access control and auditing. As a result vendors in the financial services industry connect a world wide web server to the Internet to permit customers with new account, credit card, and loan information; based on user names and passwords, Internet IP address, or domain name.

8.1 Types of Firewalls

There are several types of firewalls for different levels of security. Firewalls include simple traffic logging systems, IP packet screening routers, hardened firewall hosts, and proxy application gateways.

8.1.1 Simple Traffic Logging Systems

Traffic logging systems are the most used firewall system in Web servers. This system records a file of all network traffic that goes through the firewall for auditing goal. On most Web servers, an audit log file that lists every access of files on a given Web site. It records the name of the file accessed, the domain name that the user came in one, the exact time second of the access, and number of bytes transmitted.[16]

8.1.2 IP Packet Screening Routers

This simplest firewall is also called a packet filtering gateway. The screening router operates by filtering incoming information packets and allow or refuse IP packet based on several screening rules. These screening rules are as follows:[17]

---

[12]Deborah Russell & G.T. Gangemi Sr., Computer Security Basics, (O'Reilly & Associates, Inc., 1991) 175.
[13]Deborah Russell & G.T. Gangemi Sr., Computer Scurity Basics, (O'Reilly & Associates, Inc., 1991) 176.
[14]Andrew B. Whinston & Ravi Kalakota, Electronic Commerce: A Manager's Guide, (Addison-Wesly Longman, Inc., 1997) 141
[15]Andrew B. Whinston & Ravi Kalakota, Electronic Commerce: A Manager's Guide, (Addison-Wesly Longman, Inc., 1997) 142-143.
[16]Anrew B. Whinston & Ravi Kalakota, Electronic Commerce: A Manager's Guide, (Addison-Wesly Longman, Inc., 1997) 126-127.
[17]Andrew B. Whinston & Ravi Kalakota, Electronic Commerce: A

IJCSS, Vol.1, No.1, 2009
ISSN: 1803-8336

- Incoming packet protocol. Control filtering of network traffic based on protocol (TCP, UDP, ICMP).
- Destination application to which the packet is routed. Restrict access to certain applications.
- Known source IP address. Block access to packets coming from certain IP addresses.

Firewalls consist of two mechanisms: one that blocks incoming traffic, and one that allows outgoing traffic. Both can block many security holes. For IP packet screening, many firms count on routers from companies. It is attractive to small companies because of its low cost. Routers are like barriers to most accidental Internet sponges.

8.1.3 Hardened Firewall Host

A hardened firewall host requires users to be connected to the reliable applications on the firewall machine before connecting further. That is to be protected against unauthenticated and unauthorized interactive log-ins from the outer world. There is some rules to create a hardened host system. These rules are:[18]

- Managers must take away all user accounts besides those necessary for operation of the firewall. Therefore, they destroy the security procedures.
- Managers must take away all uncritical files and unaccomplished, especially network survey programs and client programs like FTP and telnet.
- Managers must broaden traffic logging and monitoring to check remote access.
- Managers must disable IP forwarding to prevent the firewall from forwarding unauthorized packets between the Internet and the enterprise network.

A hardened firewall computer records who has logged onto a system, and who has tried to log on but failed. Therefore, the hardened firewall host provides security and a way to increase auditing power.

8.1.4 Proxy Application Gateways

Firewalls are also created through "proxy service." Application gateway is the host computer running the proxy services. Application gateway is the host computer that runs the proxy services. Application gateway takes place between the Internet and a company's internal network. Therefore, it organize traffic in both directions. It disposal firewall safely without creating a security hole for hackers to access the corporate network. Proxy servers are also used for storing or caching documents on a local server. The proxy method works by blocking incoming HTTP connections by using a packet filtering router, which allows the packets to go to the web applications only.[19]

A user who wants to connect this system must go through the following steps:[20]

- Browser must use the application gateway to talk to the Web server and provides the name of an internal host.
- The user's source IP address must be checked and accepted or rejected by the gateway according to any access criteria in place.
- The browser may need to authenticate itself by using a password.
- HTTP connection is created between the gateway and the internal host by the proxy service.
- Bytes are passed between the two connections by the proxy service, and the application gateway audits the connection.

9. TYPES OF SALES

There are three basic types of sales: face-to-face, Telephone, and Internet sales.

9.1 Face-to-Face Sales

This relationship is exchanging physical goods in physical place. People can pay paper money or coin, which is not a problem (no security problems). But if people choose to write a check, pay with an ATM card, a debit card, or a credit card, there will be a security problem. It does not ensure secure transactions, because each time you use your credit card, or debit card, you are making a transaction. Although, cash payment can not easily deny but it could be forged. A check can be dishonored by the bank and problems may appear when using a credit card, if the person is careless, other parties can obtain the credit card number, and use it to run up their charges.

9.2 Telephone Sales

This risky sale is not in a store. Parties have less knowledge about each other. There is a time gap which means many things can go wrong. Impersonation is easier over the telephone. Both parties can not identify each other, can not verify signatures which makes it easier to use stolen credit card numbers, the people who got your credit card number over the telephone can use that credit card number to run up their charges.

9.3 Internet Sales

Internet sales take two forms: ordinary commerce in material things and information commerce. Ordinary commerce is like any common transaction but there is no physical presence, or identification to each party. Information commerce is more like face-to-face transaction but with little electronic identifying exchange is needed: the buyer will send digital cash, and the seller will send information. Microcommerce in information will require inexpensive participation of a third party such as credit card issuer.

In summery, I think that transactions through the Internet are more secure than transactions over the telephone. Transactions over the Internet if not more secure than face-to-face sales using credit, or debit cards it is as secure as it. Still people trust transactions over the telephone and do not trust transactions through the Internet.

10. CONCLUSION

In this study we showed by conducting an empirical study that our hypothesis is true, and that lack of security on the Internet is the leading reason for people not to make more transactions through the Internet, although it was not strongly proven to be distinguished from some other reasons. Current Internet technology offers a decent level of security that people do not

Manager's Guide, (Addison-Wesly Longman, Inc., 1997) 127-128.
[18]Andrew B. Whinston & Ravi Kalakota, Electronic Commerce: A Manager's Guide, (Addison-Wesly Longman, Inc., 1997) 128-129.
[19]Andrew B. Whinston & Ravi Kalakota, Electronic Commerce: A Manager's Guide, (Addison-Wesly Longman, Inc., 1997) 129-130.
[20]Andrew B. Whinston & Ravi Kalakota, Electronic Commerce: A Manager's Guide, (Addison-Wesly Longman, Inc., 1997) 130-131.

know about. In order to attract more people to make transactions through the Internet that technology has to be demonstrated. People should know that there is nothing to be afraid of, and that making a transaction on the Internet is even more secure than making it over the phone. To ensure security on the Internet, several methods have been developed and deployed. They include firewalls for perimeter security, authentication of users and servers, encryption, and data integrity.

Transaction security is critical, without it information transmitted over the Internet is susceptible to fraud and other misuse. However, just having secure transactions is not enough for business. Merchants or sellers must address all Internet security concerns. Online firms must take additional precautions to prevent security breaches. In order to protect consumer information, merchants or sellers must maintain physical security of their servers and control access to software passwords and private keys. Techniques such as secret and public key encryption and digital signatures play a crucial role in developing consumer confidence in electronic commerce.

11. REFERENCES

[1] Commerce By Numbers.
http://www.computerworld.com/home/Emmerce.nsf/All/index

[2] Electronic Commerce-An Introduction.
http://www.ispo.cec.be/ecommerce/introduc.htm

[3] Electronic Commerce on the Rise "Research Survey".
http://www.commerce.net/news/press/121197 html

[4] Barnes, J. (2007). E-Commerce and V-Business. Butterworth-Heinemann.

[5] Gangemi, G.T. Sr. & Lehtinen, Rick (2006). Computer Security Basics. O'Reilly Media, Inc.

[6] Gasser, Morrie (1988). Building a Secure Computer System. New York: Van Nostrand Reinhold.

[7] Hawker, Andrew. (2007). Security and Control in Information Systems. Taylor & Francis.

[8] Kalakota, Ravi & Whinston, Andrew B. (Ed.) (1997). Readings in Electronic Commerce. Addison-Wesly Longman, Inc.

[9] Trcek, Denis. (2005). Managing Information Systems Security and Privacy. Springer.