Consumer Trust & Security in E-Commerce Businesses

This study examines consumers' concerns in regards to trust and security in electronic commerce businesses and how businesses can achieve an acceptable level.

Roberto W. Mosquera
School of Computer Science and Information Systems
Pace University
robwm77@yahoo.com
July 11, 2003
IS 692 – Research Project Seminar – summer 2003
Professor Linda Jo Calloway

TABLE OF CONTENTS:

Abstract:

The lack of trust and security between consumers and businesses has been cited as one of the major problems in the understanding of e-commerce. Privacy and security concerns are the number one reason Web users are not purchasing over the Web. This study investigates the trust and security issues of online consumers in order to establish an agreement between online consumers and online businesses.

Many consumers are suspicious about the functional system of electronic commerce, its in transparent processes and effects. Trust is seen as separate but potentially coexisting mechanism for reducing the uncertainty and difficulty of transactions and relationships in electronic markets. The analysis focuses on conditions of e-commerce transactions that are relevant for the formation of trust problems.

A survey was distributed where participants answered questions in regards to their concerns when making an online purchase and their perceptions of online businesses.

Finally, the implication is that the successful e-commerce businesses will be those who use their resources and efforts to make certain those consumers' concerns are effectively dealt with. There are various actions and means that are explained that e-commerce businesses can use to establish and preserve trust.

Introduction:

The lack of trust and security between consumers and businesses has been cited as one of the major problems in the understanding of e-commerce. Privacy and security concerns are the number one reason Web users are not purchasing over the Web. This study investigates the trust and security issues of online consumers in order to establish an agreement between online consumers and online businesses.

Trust is a central factor in interpersonal interaction. Trust reduces the financial cost of transactions and makes the joint effort more pleasant. For distant interactions, trust becomes even more important. Interactions that are carried out over long distance and that involve technologies that are poorly understood carry more risk than face-to-face interactions.

In the process of e-commerce, necessary information essential to the completion of transactions moves from site to site. Nonetheless, there are concerns that the data is susceptible to security breaches and misuse. Consumers have no need of visual identification when they give their personal and credit card information. Online businesses that disclose to be reliable, dependable and able to deliver can appear and disappear in an instant.

The aim of this paper is to find out what fixed ideas consumers have regarding the usage of electronic commerce and whether consumers are open to electronic commerce as a possible method of business. This study finds that e-commerce is not a preferred method of transacting business because of security concerns and consumers are not aware of security measures that should be established by business. This paper recommends that the industry undertake an education process for consumers to remove some of the unknown fears in e-commerce and that consumers are made aware of methods to avoid e-fraud.

From the survey, 85% of the participants (17 out of 20) stated that their main concern was "security of payment (giving your credit card #). The second highest concern was "reliability of merchant" (45% 9 out of 20).

The participants consisted of friends, and co-workers from The Bank of New York. Each was given the survey and asked to answer the questions as they saw fit. Each participant was informed of the study's purpose, survey's purpose, and assigned a "respondent number" as their identification in order to keep confidentiality.

In the next section, relevant literature is reviewed on the concept of consumers' trust and security concerns in e-commerce web sites. Then the study performed is described, where participants were asked to answer a survey on their trust and security issues of e-commerce web sites. Finally, the findings and recommendations for future studies are discussed in order to establish trust in consumers and to increase electronic transaction potential.

Review and Synthesis of the Literature:

Privacy and security concerns are the number one reason Internet users are not purchasing over the Internet. These are the main impediment to shopping on the Internet. In this information age, technology is invading private space and controversies about spam and cookies are just a few of the ongoing threats and problems experienced by online information technology users.

The main reason why consumers are hesitant to shop online is due to the lack of confidence that presently exists between the majority of online businesses and consumers. As Grabner-Kraeuter (2002) reported that, "In essence, consumers simply do not trust most Web providers enough to engage in relationship exchanges with them." Trust plays a critical role for the growth and development of e-commerce. It is necessary to study the issues that are important for the appearance of trust problems in dealings between online businesses and consumers. Buying on the Internet introduces various risks for consumers, including that of the transaction process itself being risky. And so trust is of importance to the consumer as "it reduces information complexity and lowers the perceived risk of a transaction" (Grabner-Kraeuter, 2002).

The development of trust is based on the personality and behavior patterns of the individual, his/her willingness to trust, his/her experience and that of others with the reliability of another party or system.

Online consumers can encounter either system-dependent uncertainty or transaction-specific uncertainty (Grabner-Kraeuter, 2002) when exchanging information online. Performance flaws or security problems cause system-dependent uncertainty in information and communication systems. Transaction-specific uncertainty is evident during the behavior between the consumer and the business/system interact during the online transaction. The transaction will be smooth and secure based on the functioning of the hardware and software used as well as the data exchange services used. Other technical flaws can surface in the desktop of the consumer, server of the online business and the banks involved in the transaction. The consumer can only control transactional security of his own system, but not those of others involved in the transaction.

The state in which online-transactions take place requires that businesses focus on dealings and guidelines to develop and preserve consumer trust. Kamthan (1999) declared that with the secrecy of e-commerce, the corrupt could create and/or steal identities easily through the Internet with ease. This makes it important that consumers know that companies disclose and follow certain business practices. Without such information and assurance from the company, consumers could face an increased possibility of loss, fraud, or unfulfilled expectations.

While much of the hype about Internet security has been focused on consumers who use credit cards to make online purchases with their credit cards, false or unaccredited orders make up about one-sixth of all attempted purchases on the Internet (Udo, 2001). Other security fears are of break-ins and technology disturbance, stalking, impersonation, identity theft, and computer hacking.

There are different types of personal information that is sent from a consumer to an e-commerce web site. Consumers fear that their information may be sold to third parties without permission or prior notification. As Adams (2000) stated that, consumers "fear they are being sold down the river whenever they visit healthcare—related Web sites." Information often sold has been consumers' activities on the web that is often stored in "cookies." Because of consumers' personal information such as these, is that web sites should implement secure measures.

When a user surfs the Internet, it leaves a trail that is saved in a file called a "cookie," that is left on the computer's hard drive on the user's first visit to that site. Also, as stated by Udo (2001) that a 1999 report from the USA Federal Trade Commission said, "When a user enters a chat room discussion, leaves a message on a bulletin board, registers with a commercial site, enters a contest, or orders a product, he/she directly and knowingly sends information into cyberspace." Since web sites can collect information directly or indirectly, they can build up a complete profile of an individual.

According to Udo (2001) users can protect their privacy by: not revealing personal information inadvertently; turning on cookie notices in their Web browser; being conscious of Web security; examining privacy policies and seals; using encryption; among others.

It is believed that "the longer consumers remain online, the more likely it is that they will make a transaction online" (Cox 2003). And if the transactions made are safe and successful, it will increase the comfort level of the consumer in that web site. The consumers' concern about the usage of their personal information has a major effect on their willingness to do their business online.

Consumers would trust more in e-commerce web sites if the site: is professionally built; the organization of the information has been carefully designed; the site is easy to navigate and use; the site answers consumers' questions; and the consumer is familiar with the company. Consumers look for certain components in an e-commerce web site. Those components are: "seals of approval, brand, navigation, fulfillment, presentation, and technology" (Sisson 2000). If all this information were provided, then consumers would trust an e-commerce web site more.

Companies have to establish a certain amount of trust with customers, in order to make the Internet a workable business channel. Consumers are becoming aware of the fact that many companies are now in the business of collecting consumer information and using it for marketing purposes or monitoring consumers in a way that could be perceived as invasive.

Because of privacy fears, many people continue to turn away from online commerce. This is especially the case when it involves sending out personal information. In a recent IBM survey, 61% of U.S. consumers reported shying away from a financial Web site because they were unsure of how their personal information would be used (*Building Trust in eCommerce,* 2003).

Companies can establish a climate of trust with consumers by clearly stating their privacy policies on security and encryption. Companies should ask for only necessary information of consumers and provide good communication with them as well.

As the article “Building trust in eCommerce” (2003) states, “If companies don’t create trust in eCommerce by improving privacy and security, then consumers will limit their involvement.”

Companies can accomplish this by having certification authorities, a privacy policy, and by using either SSL (Secure Socket Layer) or SET (Secure Electronic Transaction) used in their web site and technological infrastructure. “Both S.S.L. and S.E.T. are widely known communication protocols, each providing a way to make payments over the Internet” (Grabner-Kraeuter 2002).

SSL technology is the standard protocol for secure, Web-based communications that allow businesses to communicate safely with any consumer using any of today’s e-mail programs. According to Performance Computing Magazine (*Your step-by-step guide to Ecommerce,* n.d.), there are four main benefits over SSL that SET offers. Businesses have assurance that transactions will not be falsely charged back, helping to reduce the risk of e-commerce adding unexpected costs. For consumers, SET confirms them that they are dealing with a legitimate business and that their credit card number can’t be stolen and/or intercepted. SET also offers lower fraud rates and therefore keeps costs down. However, SET is more expensive to install than SSL because it requires software to be installed with the consumer, the merchant and the bank.

Furthermore, many businesses are seeking out seal programs, such as TRUSTe and Better Business Bureau OnLine. These seal programs show a better acceptance among Web businesses that privacy and security policies are necessary.

Sisson (2000) described that there are 6 main components of an e-commerce site that suggest trustworthiness:

Seals of Approval - Symbols, such as VeriSign and MasterCard, designed to re-assure the visitor that security has been established.

Brand - The business's promise to deliver high quality and credibility based on its reputation and consumer's experience.

Navigation - The ease of finding what the consumer is searching for.

Fulfillment - Clearly indicates how orders will be processed, and provides information remedies if there are problems with the order.

Presentation - Web design that suggest quality and professionalism.

Technology - Up-date-technology that also suggest quality and professionalism.

According to Friedman (2000), there are 10 trust-related characteristics of online interaction that is helpful in analysis and design work.

1 - Reliability and security of the technology - Technology that is not yet 100% reliable or secure.

2 - Knowing what people online tend to do - Users (especially consumers) fear viruses, hackers, and other users in disguise.

3 - Misleading language and images - Designers using misleading language and images to suggest to users better reliability and security in the technology.

4 - Disagreement about what counts as harm - Assessing the harms that may take place from breaches of trust.

5 - Informed consent - Letting users know that private information may be store ("cookies") or used for marketing purposes.

6 - Informed consent involves telling users of the potential harm or benefit of an online interaction and giving them the explicit opportunity to consent or decline to participate in the interaction.

7 - Anonymity - The absence of identifying information associated with a communication.

8 - Accountability - The need to know the person you are interacting with.

9 - Saliency of cues in the online environment - The existence or absence of signs in the web site can increase or decrease user confidence in the source.

10 - Insurance - Insurance refers to the compensation of individuals for any future harm was to occur.

Although there are many shocking stories about identity theft and other crimes online, "American consumers are more trusting when conducting Internet transactions now than they were a year ago, according to a new study called the 'Consumer Internet Barometer'" (Cox, 2003).

According to a report, produced by NFO WorldGroup, Forrester Research and The Conference Board, "More than 33 percent of consumers polled express trust that their online financial transactions are safe, up from 27.5 percent a year ago" (Cox, 2003). Also, one-fourth of consumers trust that their private information will be protected when purchasing online, up from 21.9 percent a year ago.

"Consumers' concern about privacy of their personal information has a significant influence on their willingness to engage in business exchanges online," said Lynn Franco, director of the Consumer Research Center of The Conference Board. "But this trust barrier is beginning to erode." Cox (2003) stated that according to comScore Networks, online consumer sales are on track to reach an estimated $74 billion for 2002, an increase of nearly 40 percent over 2001. As stated by Cox (2003), comScore stated that "convenience, novelty and efficiency, an increase in the number of new online buyers, and greater spending among experienced buyers" were the key drivers to the increase.

comScore also stated that in a recent study, "38 percent of Internet users reported that to some degree, they are still uncomfortable providing their credit card information on the Internet. And 36 percent report they worry about the security of financial transactions. Another 40 percent say they are concerned about privacy when they shop online" (Cox, 2003).

Businesses can develop trust with consumers in the Internet by "taking advantage of their good reputation, references or image transfers from real-world brands when addressing new customers via the Internet" (Grabner-Kraeuter, 2002). And those businesses that lack good reputation can compensate it "by investing in trust developing measures and signaling activities" (Grabner-Kraeuter, 2002).

For the reason that in the nearby future trust will remain the key factor for success or failure of e-businesses, it is very important for Internet companies to act in a way that encourage consumers' trust. Attempts to increase the security of e-commerce systems and trustworthy ways of online businesses will prove to be of benefit for both consumers and companies dealing with e-commerce.

Summary of important issues and research questions:

What would make consumers trust in e-commerce web sites more? How do consumers evaluate a web site's security and privacy?

Consumers would trust more in e-commerce web sites if the site: is professionally built; the organization of the information has been carefully designed; the site is easy to navigate and use; the site answers consumers' questions; the consumer is familiar with the company. Consumers look for certain components in an e-commerce web site. Those components are: "seals of approval, brand, navigation, fulfillment, presentation, and technology." (Sisson 2000) If all this information were provided, then consumers would trust an e-commerce web site more.

Do consumers believe that transactions made in an e-commerce web site is any less secure than the current data transfer processes consumers regularly use?

It is believed that "the longer consumers remain online, the more likely it is that they will make a transaction online." (Cox 2003) And if the transactions made are safe and successful, it will increase the comfort level of the consumer in that web site. The consumers' concern about the usage of their personal information has a major effect on their willingness to do their business online.

What is sensitive about the data in the transmission that requires implementing secure measures?

There are different types of personal information that is sent from a consumer to an e-commerce web site. "Consumers who fear they are being sold down the river whenever they visit healthcare—related Web sites" (Adams 2000). They fear that their information may be sold to third parties without permission or prior notification.

Information often sold has been consumers' activities on the web that is often stored in "cookies." Because of consumers' personal information such as these, is that web sites should implement secure measures.

How can companies establish and maintain a climate of trust with consumers?

Companies can establish a climate of trust with consumers by clearly stating their privacy policies on security and encryption. Companies should ask for only necessary information of consumers and provide good communication with them as well. Companies can accomplish this by having certification authorities, a privacy policy, and by using either S.S.L. or S.E.T. used in their web site and technological infrastructure. "Both S.S.L. and S.E.T. are widely known communication protocols, each providing a way to make payments over the Internet" (*Your step-by-step guide to Ecommerce*, n.d.).

Description of the Pilot Study:

The Study

The study was qualitative as it was primarily concerned with getting a subjective "fee" for the research topic. It was decided that due to the length in time of the class – 6 weeks – the pilot study would be conducted with a survey. The survey was subjective as it was assumed that e-commerce web sites are not that trustworthy or not so secured.

After browsing through the Internet, a survey was found were the questions were similar to those that wanted to be asked. A version was created, but it was lengthy – three and a half pages. A co-worker was asked if she would answer such a survey. Her answer, "No!" After further modifications, it was brought down to two pages. The survey consisted of several questions using the "likert scale." Yet, this version was also thrown out and a final version was created that consisted of six short-answer questions on one page.

The participants of the survey included friends and co-workers from The Bank of New York. Each was given the survey and asked to answer the questions as they saw fit.

Participants replied to a survey that contained questions on a that asked of their online shopping experience and their trust and security concerns in e-commerce web sites. The survey was distributed personally on a one-page paper.

The following questions were asked:

- Have you ever made an online purchase? If yes, how was your experience? If no, why not?

- What are your main concerns with using the Internet to purchase a product/service?
- What makes you think the making an online purchase is less secure than the current process you use to make a purchase?
- Do you believe that what an e-commerce web site states is true and factual? Why/why not?
- Do you usually find out how an e-commerce web site will use the information submitted by you? Why/why not?
- Do you feel that an e-commerce web site matches your goals/priorities in making a purchase? Why/why not?

Individuals were asked to participate in the survey voluntarily and were informed of both the survey's purpose and study's purpose. Each survey participant was then randomly allocated a "respondent number" for identification and to maintain confidentiality.

The completed survey was returned within that same day, most of the time within minutes.

There were 20 completed surveys returned out of the 20 distributed. 1 of the respondent was surveyed through a phone interview. The answers were written by myself.

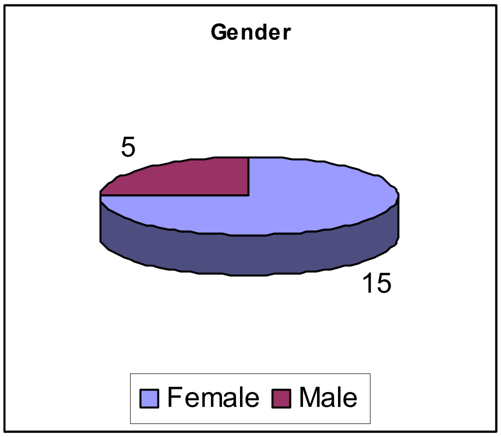
Limitations of this Study

Participants included in this study were limited to close personal friends and co-workers from The Bank of New York. There was no data acquired to acknowledge the background of any of the participants as the majority of them were female (75%, 15 out of 20) and it would be irrelevant to the results as it is not a good reflection of the general population and the research was not geared towards women's concerns. Due to the timeframe available during the 6-week class, there was little time to collect a much larger and diverse sample of the population. Therefore, this sample may not be considered a good representation of the general e-commerce population.

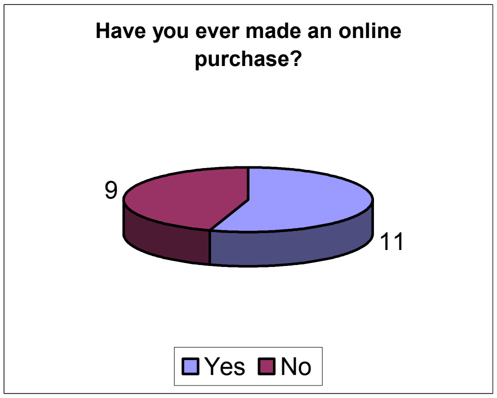
How a Complete Study Would Be Carried Out

A complete study would be organized and carried out much more differently than the one performed here. The sample would be much larger – in the hundreds. The survey would be placed in the Internet to obtain such a large sample, to make it easier to distribute the survey, and to save paper. The survey would also have a few more questions and acquire data to acknowledge the background of the participants, as it would be diverse and relevant.

Findings:



The Pilot Study consisted of 75% (15 of 20) female and 25% (5 of 20) male.



Based on Question #1 of the survey ("Have you ever made an online purchase?"), the Pilot Study found that 55% (11 of 20) of the participants have shopped online before, while 45% (9 of 20) of the participants have never done so.

Respondents' reasons **FOR** purchasing online:

"It was quick and hassle free, no line, not waits." – respondent #5

"It was great, no lines, no crowds, and especially at Christmas time the best time to go shopping." – respondent #11

"It is good to make an online purchase because I can save on the tax and sometimes the price of the merchant is cheaper." – respondent #15

"The advantages are that consumer does not need to go to the store to buy the merchandise and mostly it is for free. It is more convenient to compare the price of goods among different web sites so as to select the store with the most reasonable price (not the cheapest price). The disadvantage is shipping fees (I actually shop where there is free shipping)." – respondent #16

"It was ok, price made up the time differential." – respondent #19

Respondents' reasons **FOR NOT** purchasing online:

"I have not purchased anything online because I have the fear of losing my credit card number." – respondent #1

"I am not interested, have no time." – respondent #3

"Because I like to look at the merchandise before purchasing. Sometimes what you see online is not what you get. Well, that's my main concern." – respondent #4

"Security and forged identity." – respondent #14

Sample of respondents' answers to Question #3 of the Pilot Study:

"What makes you think the making an online purchase is less secure than the current process you use to make a purchase?"

"With the current process of purchasing merchandise I can pay with cash or check. With an online purchase, I have no choice but to give my credit card #. I find this method to be insecure, especially on an online transaction." – respondent #2

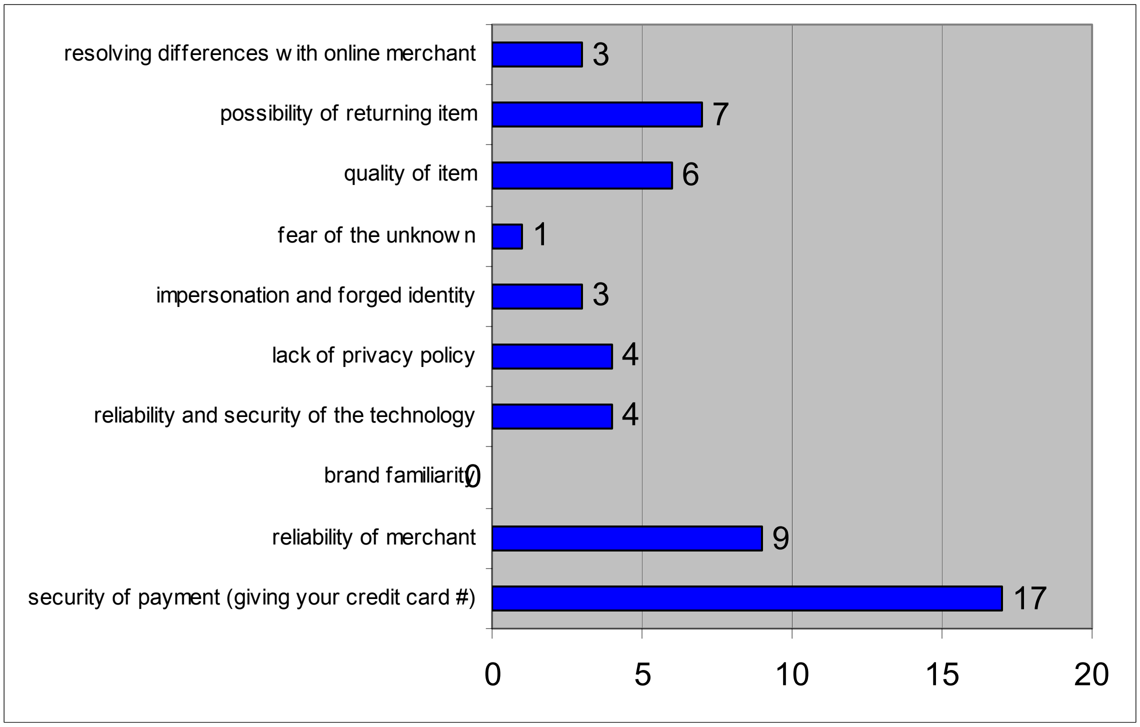
"Because you don't know what is going on while you are entering your info online. It's like being in the park and writing your info on paper and leaving it on the bench." – respondent #5

"Hackers might be able to hack into the web site and steal the credit card information." – respondent #7

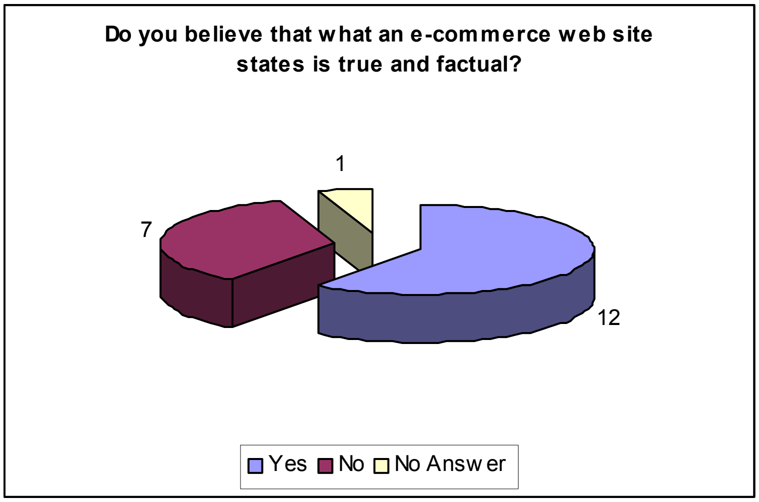
"I don't know what checks & balances they have to secure the info I give them." – respondent #11

"When I fill in my info and make the payment online, first things I need to know is the web sites should have "SSL Secured <128-bit>" because it can protect me when I transfer my information from my computer to the e-commerce web site." – respondent #15

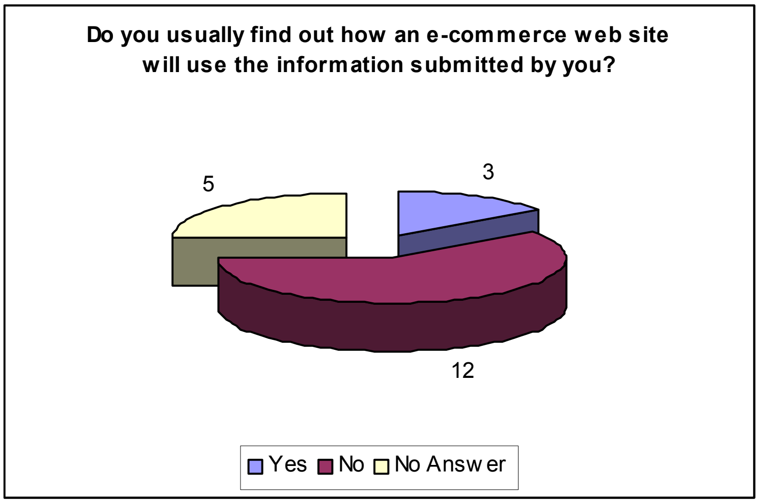
"The unknown." – respondent #18



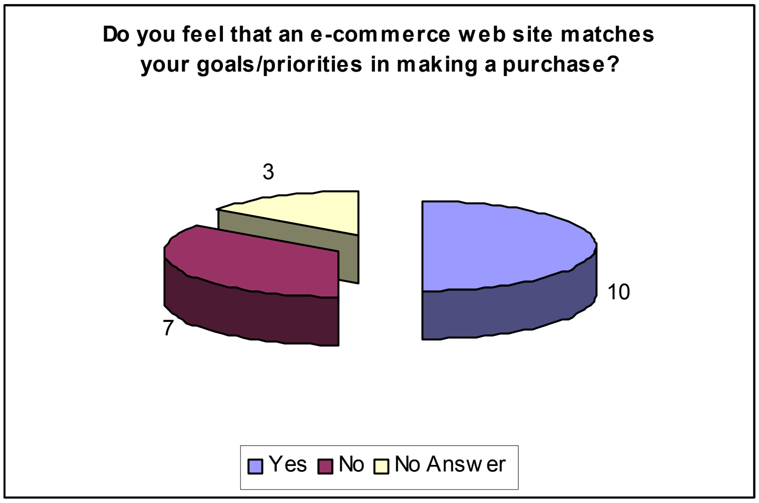
Based on Question #2 of the survey ("What are your main concerns with using the Internet to purchase a product/service? [you can choose more than 1]"), the Pilot Study found that 85% (17 of 20) of the participants state that *security of payment (giving your credit card #)* is their main concern. *Reliability of merchant* was their second highest concern. Among the least of the participants concerns it included *brand familiarity and fear of the unknown.*



Based on Question #4 of the survey ("Do you believe that what an e-commerce web site states is true and factual?"), the Pilot Study found that 60% (12 of 20) of the participants do; 35% (7 of 20) do not; and 5% (1 of 20) did not have an answer.



Based on Question #5 of the survey ("Do you usually find out how an e-commerce web site will use the information submitted by you?"), the Pilot Study found that 15% (3 of 20) of the participants actually do as they are aware of such information; 60% (12 of 20) do not at all, either because they trust the site or do not bother with it; and 25% (5 of 20) did not have an answer as many of them never shopped online and were not able to provide an answer.



Based on Question #6 of the survey ("Do you feel that an e-commerce web site matches your goals/priorities in making a purchase?"), the Pilot Study found that 50% (10 of 20) of the participants feel that it does; 35% (7 of 20) do not feel that way; and 15% (3 of 20) did not have an answer as many of them never shopped online and were not able to provide an answer.

Relating the Findings to the Literature:

It was found that when people shopped online, even though they may be concerned about their security and have a feeling that it is less secured purchasing online than in a brick-and-mortar company, they do not bother to find out how a web site will use the information that is submitted/transmitted to the e-commerce company.

Going back to the initial research questions:

1. What would make consumers trust in e-commerce web sites more?
2. How do consumers evaluate a web site's security and privacy?
3. Do consumers believe that transactions made in an e-commerce web site is any less secure than the current data transfer processes consumers regularly use?
4. What is sensitive about the data in the transmission that requires implementing secure measures?
5. How can companies establish and maintain a climate of trust with consumers?

Many participants do not bother to find out how the web site they shop in will use their personal information. Only one of the pilot study's participants (respondent #18) said, "I'll do some research or read any disclosure posted on the site." The rest of the participants either do not shop online, do not bother with finding out, are not aware of it, or felt that their information will be sold to or used for marketing purposes.

The study proofed what Grabner-Kraeuter (2002) stated, which was that, "In essence, consumers simply do not trust most Web providers enough to engage in relationship exchanges with them." Those participants who do not shop online just simply do not trust e-commerce businesses. I am sure if they would trust e-commerce businesses, then it would lead to the growth and development of e-commerce even more.

Several participants felt that their personal information can be stolen and lead to impersonation and forged identity. Respondent #7 said, "Hackers might be able to hack into the web site and steal the credit card information"; respondent #13 said, "There is the risk that your personal information can be stolen"; respondent #16 said, "Credit card information may be stolen by hackers"; and respondent #14 did not shop online due to "security and forged identity." Precisely as Kamthan (1999) stated, that with the secrecy of e-commerce, the corrupt could create and/or steal identities easily through the Internet with ease.

In the study, the question was asked whether the participant usually find out how an e-commerce web site will use the information submitted. A couple of them felt that it would be used for advertising of marketing purposes. Respondent #15 said, "I think they send some advertising to my e-mail only"; and respondent #19 said, "Most of the time it's sold to marketing companies." Thus there is an understanding that they may be "sold down the river" (Adams, 2000) when they visit an e-commerce web site.

Only 55% (11 of 20) of the study's participants have shopped online. In order to get more consumers to shop online companies need to improve their privacy and more importantly, their security, else "consumers will limit their involvement" ("Building trust in eCommerce, 2003)

Another way companies can accomplish trust is by using either SSL (Secure Socket Layer) or SET (Secure Electronic Transaction) in their infrastructure. "Both S.S.L. and S.E.T. are widely known communication protocols, each providing a way to make payments over the Internet" (Grabner-Kraeuter 2002). Only one participant mentioned SSL when asked, "What makes you think the making an online purchase is less secure than the current process you use to make a purchase." Respondent #15 answered, "When I fill in my information and make the payment online, first things I need to know is the web sites should have 'SSL Secured <128-bit>' because it can protect me when I transfer my information from my computer to the e-commerce web site."

The key factor for success of an e-commerce web site is to encourage consumers' trust. Efforts to boost security of e-commerce systems and display trust will benefit both consumers and companies.

Discussion:

The purpose of this paper was to establish how consumers saw e-commerce as a method of purchasing a product/service and whether they were concerned and attentive of the security measures and issues that are a fundamental part of e-commerce businesses.

It was found that there are problems in the thought of e-commerce as a safe method of business transaction. The inclination for human interaction was sought by those participants hesitant to shop or trust an e-commerce web site.

Teachings on how to read a secured web site and the consequences of using non-safe web sites need to take place. This was made evident by the fact that only one participant was aware of S.S.L. or of any other security measure. Consumers must be aware that there is no going back once the *submit* button is pressed.

The consumer is swamped about the large security problems that exist with e-commerce. Businesses should be aware of the problems they face when trying to attract consumers to use e-commerce and make it part of their business objectives to educate consumers on how to avoid these security problems. Also, consumers need to use their common sense to avoid online fraud, forgery and impersonation, so to not make choices they will later grieve.

Future Directions:

In this research, total trust on e-commerce businesses was not evaluated. For example, participants of the pilot study were not required to decide if they were willing or not to go through with an online transaction and so it was not possible to evaluate the impact that trust has on this important decision. Time spent on the Internet by consumers and the web site's navigation was also not factored into the study – like, are avid Internet users more willing to make an online purchase? Future research is needed to take these issues into account and to pinpoint the key areas that businesses need to pay attention to.

Further research may need to be done on how a web site's interface impacts an e-commerce trustworthiness and image. This study lacks these factors and has quite a few limitations. A large portion of the participants was composed of female bank employees. It is possible that their perception of trust is different from the general population because of their sex and may have less experience as other consumers. Their experience of online shopping may also be somewhat different and lead them to put emphasis on other factors. Research should be done on how the demographics of consumer affect on online shopping. Therefore, complete researches of consumer trust on e-commerce businesses would include all these factors with a much larger and representative sample of the population.

References:

1. Abgrab, Nadia J, Caldwell, Helen M, Warrington, Traci B. 2000. "Building trust to develop competitive advantage in e-business relationships." *Competitive Review.* Indiana.

2. Adams, Mark. Dec 2000. "Gaining trust, protecting privacy." *Pharmaceutical Executive.* Eugene.

3. *Building trust in eCommerce.* Ernst & Young. Retrieved June 11, 2003, from http://www.ey.com/GLOBAL/content.nsf/US/AABS_-_TSRS_-_Library_-_Building_Trust_In_eCommerce

4. *Cheskin Research – eCommerce Trust Study.* January 2000. Cheskin. Retrieved June 13, 2003, from http://www.cheskin.com/p/sm.asp?mlid=37

5. Cox, Beth. *In E-Commerce We (Sort of) Trust.* 2 Jan 2003. Ecommerce Guide. Retrieved June 11, 2003, from http://ecommerce.internet.com/news/news/article/0,,10375_1563071,00.html

6. Friedman, Batya, et al. Dec 2000. "Trust online". *Association for Computing Machinery.*

7. Grabner-Kraeuter, Sonja. Aug 2002. "The role of consumer's trust in online-shopping." *Journal of Business Ethics*. Dordrecht.

8. Kamthan, Pankaj. April 1999. *E-Commerce on the WWW: A Matter of Trust.* Internet Related Technologies. Retrieved June 11, 2003, from http://www.tech.irt.org/articles/js158/

9. Light, David A. Fall 2001. "Sure, you can trust us." *MIT Sloan Management Review.* Cambridge.

10. Reilly, Tracey. 16 Apr 2002. *Consumer Trust in E-commerce Web Sites Alarmingly Low, Consumer WebWatch Research Finds.* Consumer WebWatch. Retrieved June 11, 2003, from http://www.consumerwebwatch.org/mediacenter/launchreleaseApril1602.htm

11. Saunders, Christopher. 20 Nov 2001. *Trust Central to E-Commerce, Online Marketing.* CyberAtlas. Retrieved June 11, 2003, from http://cyberatlas.internet.com/markets/retailing/article/0,1323,6061_926741,00.html

12. Sisson, Derek. 15 Feb 2000. e*commerce | Trust & Trustworthiness.* Philosophe. Retrieved June 11, 2003, from http://www.philosophe.com/commerce/trust.html

13. Udo, Godwin J. 2001. "Privacy and security concerns as major barriers for e-commerce: A survey study." *Information Management & Computer Security.* Bradford.

14. *Your step-by-step guide to Ecommerce.* (n.d.). Image Marketing Services. Retrieved June 11, 2003, from http://www.ecomcity.com/create.html

Appendix:

Sample Survey

Participants' Surveys

Summary of Participants' Surveys

Presentation Slides of Research

Survey on Consumer Trust & Security in E-Commerce

Respondent #: _________

1 - Have you ever made an online purchase? If yes, how was your experience? If no, why not?

2 - What are your main concerns with using the Internet to purchase a product/service? (you can choose more than 1)

- □ security of payment (giving your credit card #)
- □ reliability of merchant
- □ brand familiarity
- □ reliability and security of the technology
- □ lack of privacy policy
- □ impersonation and forged identity
- □ fear of the unknown
- □ quality of item
- □ possibility of returning item
- □ resolving differences with online merchant

3 - What makes you think the making an online purchase is less secure than the current process you use to make a purchase?

4 - Do you believe that what an e-commerce web site states is true and factual? Why/why not?

5 - Do you usually find out how an e-commerce web site will use the information submitted by you? Why/why not?

6 - Do you feel that an e-commerce web site matches your goals/priorities in making a purchase? Why/why not?