UNIVERSITY OF GOTHENBURG

E-commerce

A study about trust and security within E-commerce

Anil Haidari
Khushal Paktiani

Acknowledgements

We would like to sincerely thank our supervisor Faramarz Agahi for his valuable guidance and advices.

We would also like to express our truthful appreciations to our respondents who have answered this study's interview question.

Gothenburg, Sweden
March, 2011

Anil Haidari   Khushal Paktiani

Abstract

E-commerce (Electronic commerce) is growing extremely fast and getting much more in use, compared with other types of businesses. This growth is supported by spreading of Internet usage around the globe. However, the question of security and trust within e-commerce has always been in doubt. The technology is being improved day by day, which is a positive fact, but at the same time this improvement creates more and more issues as well. This study generates general knowledge about e-commerce. This study specifically gives an overview to understand different factors about security and trust between companies and their consumers. This study also mentions that security and trust work parallel and close to each other. If a consumer feels that an online deal is secured and they can trust the seller, it leads to a confident e-commerce's trade. The main focus of this study is to find out a suitable way to resolve security and trust issues that make e-commerce an uncertain market place for all parties.

This study uses the interview method in order to gain the result the study seeks. The study's empirical data is based only on interviews with four different companies that do businesses online. In order to have full glance on various sorts of companies, two interviewed companies are Web shops' supplier and two others are Web shops.

After having the result of study's empirical research, the study realized that there are some methods used within e-commerce that contribute trust and security, but still there are many security and trust issues, which need better solutions in order to gain a secure and trustworthy e-commerce for all parties that are involved in online businesses. The results also shows that within some companies the required competence for having a secured e-commerce is not there, and that some companies are overconfidence about the security of their system.

Key words: E-commerce, Trust, Security

The authors: Anil Haidari
              Khushal Paktiani
Supervisor: Faramarz Agahi
Bachelor thesis: 15 credits

Table of Contents

1. Introduction

This chapter introduces the background of the study, the problem area, purpose of this study and the study's research questions and in order to initiate the reader in this research.

There has been always barriers and problems caused by different reasons in the world of business. Internet has a very significant role in today´s trade activities. Many companies use the option e-commerce as the only way of doing business or one of the ways. As the use of e-commerce grows, so do the barriers and problems within e-commerce. The issue of trust and security is a very discussed, important and unsolved factor in e-commerce. Many, both private and entrepreneurial, consummates do not feel either secured or assured by doing business or personal purchase within e-commerce. This lack of trust and security brings some serious barriers in e-commerce, which should be seriously considered.

According to Forrester research's, an American independent technology and market research company, survey they United States had more than $ 100 billion sales through e-commerce at end of 2002. The outcome of 2002 meant a loss of $ 3 billion within e-commerce for the United State. The main reason for this cut down was the lack of trust doing businesses online. The consumers did not feel secured either about their personal information on net or the security of their credit cards number. Forrester research means that privacy statement is very important for every online site and still almost 50% of Web sites where e-commerce take place have no privacy statement at all. (Moores & Dhillon, 2003)

Even though, legislation in many countries tries to reduce the cheating or misuse of credit cards, still, by using credit card, consumers take their chances while doing business online. Legislation raises the assurance of consumers but possibility for fraud is never removed. (Ibid)

A significant survey, which took place in United States between educators and practitioner, was about the security issues in e-commerce. The survey's result showed that most of educators and practitioners were worried about their online payment and personal information, because the lack of trust regarding the security issues within the e-commerce. They were even unhappy to get unpleasant long mailing list from different places, which could cause variants of virus attack, spreading of their personal information and their credit card number. (Carr et al., 2010)

Security and trust issues could be found both within companies that engaged with small businesses and companies doing broader businesses. Jonathan (2003) means that the criminals often try to crop the information of the online consumers by establishing so called "spoof sites", which are fake Web sites. He means that such Web sites are being created by using the HTML code of the Web sites that are legitimate. By doing this the criminals manage to create a site that exactly looks like the legitimate businesses' site. Further the author means that the criminals could misuse the consumers of that Web site

by different ways, like sending them e-mails with false information in order to gain consumers' personal information. He means that the whole process could end up with criminals tricking the consumers and get access to their financial accounts and so on.

1.1 The Background of E-commerce

Often, 1990s comes up directly in people's mind when they think of e-commerce, because it was a time when e-commerce had a good development. According Dykert et al. (2002) the e-commerce's start is way earlier than the 1990s. The authors mean that e-commerce had always, and still have, strong connection with the Internet, and the e-commerce's start goes back with the Internet's establishment that started with a military research project under the 1970s. The name of the project was DARPANET (Advanced Research Project Agency Network) and its aim was secured communication. After a good result of this project four universities in USA got the responsibility of developing the idea in order to exchange the research results, in a secure way, between the universities.

Further the authors claim that the first e-mail was sent in the 1972, and after that, eventually, the connection between USA and Europe was created online. According the authors, it was this connection that made e-commerce a reality for most of the branches. After that e-commerce began to develop slowly until the beginning of 1990s. Dykert et al. (2002) mean that it was at the beginning of 1990s when e-commerce had its successes. It was then when many opportunities were given within e-commerce for the different businesses. The authors mean that one of the reasons why e-commerce had its successes at the beginning of 1990s was www (World Wide Web) that was introduced in 1992.

1.2 Purpose and research question

The purpose of this study is to create a general knowledge about the e-commerce. Further the main purpose of this study is to look up at the issues regarding security and trust within e-commerce. Moreover the study's purpose is to look up at the factors that improve the security and trust within e-commerce.

The research question of this study has its focus on security and trust within e-commerce and is divided into three parts, which are as following:

- Which factors create common security issues within e-commerce?

- Which factors create mistrust among the consumers of the e-commerce?

- Which solutions can be used to prevent/reduce security issues within e-commerce and how to create trust among the consumers?

1.3 Delimitation

There are many factors that are important within e-commerce, which should be improved. But considering our limited resource we have chosen to focus on security and trust within e-commerce. The study is limited to only e-commerce companies, i.e. trust and security issues and solutions for them would be studied from business to consumers' (B2C) perspective. This study will be about finding ways to create trust and security for consumers while doing businesses within e-commerce. As e-payment issue is one of the most important factors within e-commerce, this study will have a minor focus on it as well.

1.4 Disposition

The second chapter describes the methods that have been used in this study in order to get a practical result in this study. The method which is used in the study is a qualitative study in form of interviews with several companies. Further, the third chapter is concerning the literature study where the various well-known theories are discussed, in order to provide a basis for further research. Chapter four presents the summary of interviews which have been done with a variety of companies during the study. These summaries give an overall vision of how different companies explain e-commerce security and trust. In chapter five, the study analyzes the literature study with the empirical and their relation to each other. This analyze helps the study to identify the possible similarity and disparity between the theoretical facts and companies that work with efforts with e-commerce. Finally the last chapter is conclusion. In this chapter, study links up the research's purpose with the consideration that study reaches under analyze and discussion chapters. This chapter also recommends some further researches about the chosen subject.

2. Method

This chapter presents how all the materials are collected. This chapter also explains which method has been used to gather the needed material, which are useful for this study. The methods used for the research stand of two parts, namely Literature study and Empirical study, which are presented in this chapter.

The literature and empirical study are considered to be useful for the purpose of this study, because the literature study contributes a good knowledge about security and trust issues and their solutions within e-commerce. Further to have an understanding, which is based on the reality, about the chosen subject empirical study is being done. The empirical study gathers information/knowledge about how companies experience these security and trust issues and which solutions they recommend regarding these issues. Using both kinds of methods help the researchers to continue the study in some scientific and experienced based manners.

2.1 Literature study

Patel & Davidson (2003) mean that by studying different kinds of materials for theory, which is relevant to the chosen field/subject, the awareness and basis for the wanted knowledge is to be created. A researcher could use the knowledge from theories or models, which could be found from the different literatures, or he/she could gather the wanted knowledge from the previous studies/surveys. Having the right theories contribute to a better understanding of reality. The authors mean that a theory is a system of assumptions and statements, which describes the part of reality that is to be studied. This process helps the researcher to find what is essential within the problem area, so she/he could gradually make delimitation (Patel & Davidson 2003).

The literature study of this study has been created from related literatures, scholarly articles and Internet. The literatures used in this study cover big parts of the chapter three, which is why they have been a very important help in contributing to build a good empirical chapter. Combining the gathered knowledge from literatures, scholarly articles and Internet made the chapter three very related and complete. The reason for having a combined material for the literature study is to look at the chosen subject from different perspectives and find different kinds of solutions for the study's problem area. Another reason of the combination is also to make it easier to have the most related material for the empirical study.

Searching for materials for the literature study chapter was done both online and offline. Two big well known libraries, Library of the University of Gothenburg and Library of the Chalmers, were used for finding the literatures for the subject area. The reason why these two libraries were used is that both of them have lots of useful resources, and besides the researchers of this study have used these libraries many times before and are well familiar with libraries. At first, great numbers of literatures were gathered about the e-commerce in order to get a broad overview about the subject. Then the ones about security and trust within e-commerce were chosen and the rest were kept aside for further

possible use. After doing that, a deeper look at the chosen literatures was done, in order to choose the most useful and related literatures for the problem area being studied. This process of finding literatures required many hours of searching both, online and offline. When the options to find useful literatures were out, then a great help from the library personals was offered that made the process move forward.

In addition, to find the related scholarly articles many different e-libraries and databases were used in order to have a look at different articles across the world. The same tactic, as for sorting of literatures, were used for the scholarly articles. Many articles about e-commerce were gathered from different e-libraries and databases, then most related to the e-commerce's security and trust was chosen, and out of them the most useful ones were selected. The material from Internet obviously was found from the Internet, but before using the material it was made sure that the source being used in the Web site was real and trustworthy.

2.2 Empirical study

Considering the purpose of the study and to achieve the goal of the study, the method of interview (qualitative method) has been chosen. The other methods like questionnaire (quantitative method) have been eliminated, due to not being useful for this study. Since the main focus of this study is how e-commerce's companies experience the security and trust within B2C e-commerce, it has been decided to interview only those who work within e-commerce's companies.

The researchers of this study gathered information and knowledge both about companies and related subject long before the interviews' process, in order to have a good understanding both about the companies and the subject to be talked about during interviews. The information about the companies was obtained from the companies' Web sites and the knowledge about the related subjects was acquired from the literatures, articles and Internet. Having both, the required knowledge and information helped the researchers to be well prepared to achieve a successful interview process.

2.3 Interview

The structure of interviews in this study is semi- structured. The reason of choosing this sort of interview is that it suits well the purpose of this study. According Bryman & Bell (2005), there are three different kinds of interview methods; unstructured, structured and semi structured. Bryman & Bells (2005) explain that the semi structured interview is the kind which starts with some open and general questions that follow with more specific and deep question. Respondent speaks and interviewer asks most often dissimilar questions and chooses the subject which is more related to his/her work and the respondent discuss or answers them. It can happen that respondent answer few question in the middle of his discussion. There are not any pre-structured questions. The questions are asked in the middle of respondent's discussion. The final kind of interview is the structured interview method. The questions are already fixed about a specific subject that is interesting for interviewer. This kind of interview method is mostly used with a quantitative study (Bryman & Bell, 2005)

The purpose of interviews, in this study, is to create an understanding about how security and trust of e-commerce is in reality, compared with the theoretical materials used for this study. At the beginning, the idea was to interview one company to find solution for security and trust issues within e-commerce. However after reconsidering the amount of interviews, the final choice became to interview four different companies in order to get different aspects on the subject and to have a broader understanding about the chosen subject.

All of four companies that have been chosen are directly involved with e-commerce. Two of them, www.guppi.se and www.emylittle.se, are Web shops that sell their products online. The other two, www.Starweb.se and www.startabutik.se, are the e-commerce system's suppliers for the Web shops. The reason of having two Web shops and two e-commerce system's suppliers is to get different perspective at the chosen subject. The idea is to have answers both, from experts and from those who are less knowledgeable about the e-commerce's system.

The choice of which companies to be interviewed was not exactly decided at the beginning, which made the study process very difficult and time challenging. It required lots of searching, both offline and online, to find some companies that were suitable for this study. They were contacted both by telephone calls and e-mails repeatedly, until four of them offered the time and knowledge they had. The rest of them didn't have the time or didn't want to do it, due to their company's policy.

Three of the interviews, have been carried out by telephone, due to the long distance problem and one of them has been occurred personally. In order to not lose the data from interviews and analyze it in the best way, all four interviews were recorded. The interviews took respectively 70 minutes, 58 minutes, 40 minutes and 45 minutes. All four interviews were transcribed, in order to have a useful feedback for study's result.

Company	Branch	Type of the interview	Time taken by interviews
A	Clothes	Face-to-face	70 min
B	Clothes	Telephone	58 min
C	Web shop's supplier	Telephone	40 min
D	Web Shop's supplier	Telephone	45 min

A very big disappointment through the interview process has been www.e-butik.se, which is an e-commerce system's supplier for Web shops. Since, they are an important supplier of the Emylittle.se and Guppi.se, the idea was to interview them as well, in order

to get a two side's perspective on the Web shops that have been developed by e-butik.se. Many telephone calls were made to the company in order to find someone who is willing and competent within the chosen area. At last, one of the personals from the company offered his help and asked to be called in the next week at 10:00 am.

When the promising phone call was made he could not go through the interview because he was sitting in some kind of meeting. He asked for a phone number so he could call back when he was finish, which he got. He did call back and the interview was started. He started with a short presentation of himself and the company, and when he was asked to answer the first question, which was about the company's security and trust, he just hung up the phone. He nor called back or answered the several phone calls that were made afterward. Many phone calls were made to the company, the same day and the other two following days, without getting any positive respond. Every time a phone call was made his colleagues would answer, in a very unpleasant way, and say he is at "lunch". To sum up the whole situation: a one week of time and work was wasted, due to a very nonchalant act and behavior of www.e-butik.se.

3. The result of literature study

This chapter explains the wide-ranging theories and consists of literature studies which provide the basis for this study.

3.1 Definition and classification of E-commerce

According Turban et al. (2010) the process of buying, selling, transferring and trading products, services and information via Internet is called e-commerce. The authors put light on some ways that widely explain e-commerce. They list these ways as communications point of view, commercial, business process, services, learning, collaborative and community point of view. Dykert & Lindberg (1996) mean that when customers and suppliers initiate using standardized and automated communication of trade between each other, then it is considered that the parties are engaged in e-commerce.

Turban et al. (2010) mean that many people get confused with e-commerce and e-business terms. They also explain that there are not many differences between these two terms. The authors say the term of e-commerce is expressing the transaction's conduct between two business parties, and the term of e-business refers to a wider definition of e-commerce. E-commerce, as already mentioned, describes the buying, selling of goods and services, and e-business, on the other hand, describe not only all part of e-commerce but also serving customers, teamwork with business partners, conducting e-learning and electronic transactions in an organization . Hansen (2005) claim that e-commerce's source is Internet, and it should be considered that all receiving order via telephone or fax should also count as e-commerce.

According Turban et al. (2010) e-commerce can get many structures depending on the level of transformation from offline to online. They mean the structures are depending on product/service selling's level, and the process or the delivery agent. Turban et al. (2010) explain something very interesting that has not been considered a lot. They say that if a consumer buys something online and the product is delivered to consumer's home then it is an incomplete e-commerce, but if a consumer buys an e-book, for instance, which can be used only online, then it is considered as a pure e-commerce. Since the product, the product's delivery, the payment and the usage will be all in digital form. Further the authors clarify that the companies, which are working only with electronic commerce is called virtual or pure e- organizations, even though, their main business is done in the offline or physical world. (Ibid)

In order to have a developed and better business J.E.J. Prins et al. (2002) points out that there are mainly two major kinds of e-commerce. The first is business to consumer (B2C) and the second is business to business (B2B)**.** Further they explain that, B2B deals with other business organizations, for example a company buys some machines from another company. The authors explain another kind of e-commerce as well that is called intra business e-commerce (B2E), which is not that common. As the study's focus is on (B2C), it will be explained widely. The authors clarify that Internet is a direct access

network to companies. They mean that, nowadays, it is not very difficult to get into contact with consumers. It is very rational to suppose that a user involving in business to consumer (B2C) e-commerce does not see the system as work device but the users see it as place to order some goods or services for his/her personal use. Further the authors explain that consumers are independent to choose the suitable vendors tends to be connected with. They mean that consumers use more the system and are directly engaged in the profitable trade, since consumers are using their own money, their equipment (computer), sharing their personal information. J.E.J. Prins et al. (2002)

3.2 E-payment methods

Almost every kind of business is gone global in today's age, and e-commerce is one of them. The fact that e-commerce has become so wide and global, contributes more and more complexities day by day within e-commerce. Turban et al. (2010) mean that technology has a very important role in development of the e-commerce, and at the same time they add that technology unfortunately plays a negative role as well, for example damaging e-commerce's security in different ways. A very important fact is being pointed by the authors, which is the fact that almost everyone could try to do something illegal within e-commerce. They mean that the security risks could be from a simple teenager's hacking attempt to very serious crimes like stealing classified information of the governments and so on.

Also J.E.J.Prins et al. (2002) mean that there are lots of security issues within e-commerce and try to look at the issues from a trust point of view. They mean that trust and security have a huge impact at each other, even if they are almost two different factors. According them, trust is the limit of confidence that feels about a relationship and means that trust is a mental system, which helps to diminish complication and hesitantly to promote the progress of a relationship, even under unsecure conditions. Turban et al. (2010) claim that there are many complexities within e-commerce, and J.E.J.Prins et al. (2002) give trust as one of the solutions to deal with those complexities. J.E.J.Prins et al. (2002) mean that trust could decrease not only complexities within e-commerce but also decreases complex realities for more rapidly and economically than prediction, authority or good dealing. To sum up his point regarding the importance of trust within e-commerce it could be said, among others, that trustworthy relationships between the companies and consumers create a strong competitive advantage for the company.

Further the importance of trust within e-commerce is mentioned by Salam et al. (2005). According them, even if there have been many attempts to make the Internet a credible e-marketplace, e-commerce still lacks the needed trust in order to become a very successful marketplace. The authors mean that, unlike other kind of businesses, e-commerce is a lot dependent of the consumers' trust, the trust which is not entirely gained within e-commerce. At the same time, they make it clear that mistrust within e-commerce could be easily come up and in different ways, unlike other types of businesses. They give an example of common and serious mistrust among users, which is a very big issue for the e-companies, namely the lack of trust in order to get involved with the financial

transactions, which prevents the consumers to give their credit card information to the Web sites

The security issues and mistrust caused by, among others, e-commerce being spread widely and globally, is mentioned also by Salam et al. (2005).They also agree with the fact that creating trust within e-commerce is harder compared with the offline or physical business, and at the same time they claim that it is very important that every company builds trust, the same way as trust is being created in offline or physical business, among consumers. The authors mean that despite the lack of seriousness for security and trust within e-commerce, some companies starting to consider the significant of trust and begin to think about renewing their security infrastructure to recover consumers' confidence on them. They authors mean that having security polices, which eliminate the risk of fraud and corruption and insure the consumers, is one of the ways to gain consumers trust within e-commerce. (Salam et al., 2005)

Further the authors bring up the security threats caused by not online external but also by internal factors, and mean that every company should have this in mind. They mean that computerized information about consumers and even other parties can face some threats, both inside and outside (internal and external) threats. They exemplify their statement by claiming that threats could be caused by extern hackers, employees of international organization, insufficient physical security of hard and software, not well understanding of technical factors and so on. The authors mean that companies should have a good focus on strategies that helps e-commerce with defense for such problems, for example to have a defense program, which can guarantee security of e-commerce, specially the online transactions.

According Turban et al. (2010) at the time when e-commerce established as a business process, it was very hard for consumers to trust this new process. Consumers were unwilling to use their credit card online. The authors claim, by passing time, it is much easier for consumers to get involve with e-commerce's transaction. They mean that it is mostly young people who are willing to use their credit card. However youths' purchases are very small and these small payments are called micropayments. The authors argue that online payment methods have to be secured and trusted by consumers. E-payment methods that are used with (B2C) e-commerce are:

- Electronic payments cards (credit, bill, charge)
- Virtual credit cards
- E-wallets (or e-purses)
- Smart cards
- Electronic cash (several variations)
- Wireless payments
- Stored value card payments
- Loyalty cards
- Person to person payment methods
- Payments made electronically at kiosks

According Turban et al. (2010), there are number of e-payment systems that need some particular soft or hardware in order make an e-payment process possible. The authors mention that there are some questions raise about the method of e-payments, for instance, how to make sellers to accept a specific method when there are not several buyers who are using the same method? Likewise, how to make buyers to accept a method that are not used much by sellers? Turban et al. (2010) mean that there are some factors that influence the choice of a specific method for e-payments. The authors explain that the first factor is *Independence,* which means that both payers and payees need to install specific sorts of software in order to make an e-payment's process possible. Further the authors explain the second factor, *Interoperability and Portability,* which includes all kinds of e-commerce's process that are related to other systems and supported by a standard computing policy.

Turban et al. (2010) explain that *Security* is another factor that should be considered. If the risk for consumer is higher than the risk for seller, then it is hard to make users accept this method. They mention *anonymity* that means some particular methods are made to keep buyers' identity in secret, because some buyers want to keep their identity anonym in the time of using their credit card on Web sites. The authors say *Divisibility* is another factor which claims that some payees accept only those credit card purchases which are neither very small nor very huge like millions. According authors, *Easy to use* is very useful when it comes to business to consumer (B2C) e-payment system. They claim that credit card is the best way to use in order to make the process easy for both parties. Further the authors explain the *Transaction fee*, which explains that with every credit card payment, the seller pays a transaction fee that is up to 3 percent of the product's price. That is why most of sellers do not accept very small purchases. Finally, the last factor is *Critical mass* which means that, a significant number of traders should accept the payment methods.

3.3 Problem with Security and Trust

As people think of security issues within e-commerce they often think of just different types of cyber attacks, but security issues within e-commerce consists of many other factors than just cyber attacks, mean Turban et al. (2010). The authors give a good example of one main issue within e-commerce, namely the sensitivity of personal information. For example when a consumer wants to buy some literatures online and he/she is asked for some demographic and other personal information to fill while ordering the literatures online. The consumer refrains from the purchase of litterers because he/she does not want to give out his/her personal information on the Web site, due to the lack of trust. The authors name another serious issue within e-commerce that almost every company faces, which is to make consumers believe that the Web site is real and not fake. How to prove for the consumers that the Web site is totally legitimate and legal? Turban et al. (2010) on the other hand mention problems that could be caused by consumers, for example if consumers send a bad check or don't send it at all, and later refuse the sending of the bad check or argue that they have paid right, how the company disprove the denial?

Although awareness of security issues has increased in recent years, according Turban et al. (2010), organizations continue to make some fairly common mistakes in managing their security risks; *undervalued information* is one of those common mistakes, which most organizations make, mean the authors and claim that there are few organizations which have a clear understanding of the value of specific information assets.

Narrowly defined security boundaries, is another common mistake mentioned by the authors, which is done often within e-commerce organizations. They mean most organizations focus on securing their internal networks and fail to understand the security practices of their supply chain partners. Further they add that many organizations are reactive rather than proactive, which means focusing on security after an incident or problem occurs. This kind of mistake is called *reactive security management*. Another very common mistake is, *dated security management process,* which means that organizations seldom update or change their security practices to meet the new security threats. Such companies rarely update the knowledge and skills of their staff about best practices in information security. And finally the authors name a very common mistake done within e-companies, which is *lack of communication about security responsibilities* which means that security issues often are viewed as only an IT problem, not an organizational issue.

Further Turban et al. (2010) bring up some other serious mistakes, which are not that common as the mistakes mentioned in the above paragraph. They mean that many companies do not have a good consideration about the factors like *authorization, auditing, integrity and nonrepudiation*. To illuminate why carelessness of these factors could resulted with problems within e-commerce, the authors briefly explain the meaning of these factors. According them, authorization means to have the right to get access to some resources, which could be done both by persons or programs, and if it is done for the wrong purpose or by someone unauthorized it could "kill" consumers' trust. Further the authors mean that auditing is a process of the collecting of information about particular resources. In this process information, which is not wanted to be shared, could be shared, and this will cause mistrust for the companies. The authors continue and signify that many companies do not value the importance of the factor integrity, which could results to the fact that the data under the whole process of data transiting could be changed or damaged. The authors further mean that it is not so unusual that people/organisations try to do transactions that are not lawfully, due the carelessness of the companies regarding nonrepudiation.

Nonrepudiation is a process that prevents such actions. It makes sure that lawful transactions take place. However, Turban et al. (2010) mean that security and trust issues could be seen differently by different parties, i.e. companies and consumers. The authors shortly present the different perspectives of issues experienced by parties, which are mentioned bellow:

- *From the company's perspective*

   The security issues do not just concern the users, they also concern the companies. For example, some users might try to break into the Web server and change pages and

everything the site contains. Or maybe the user tries to change the availableness of the server, so it is not available to everyone, or similar problems.

- *From the user's perspective*

The first question the user thinks of might be the seriousness of the Web server, if it is owned and ran by a company that is legitimate. The user could also be unsure about the codes and content of the page and the form he/she is filling, if it contains some despiteful or unsecure threats for the user. Users are always concern about their personal information, which makes them wonder how they can be sure if the Web server will not share out their information to some other unrelated party.

- *From both parties' perspectives*

There are some other factors that concern both of the parties, the company and the user, for example, the network connection. How can both parties know if the net connection they are using is totally free? A third party could be involved in the network connection they are using and share both sides' information. The information sent between the user's browser and the company's server could be changed under the process, without either of the parties knowing it.

3.4 Solutions for Trust

As trust is a very important factor in order to gain consumers' beliefs to make e-commerce totally a trustworthy marketplace, some factors are presented as solutions for the trust issues within e-commerce. First *four trusting belief*s, by Salam et al. (2005), are presented then *Seven critical factors that affect trust* by Ofuonye et al. (2008).

3.4.1 Four Trusting beliefs

The first trusting belief presented by Salam et al. (2005) is *Belief in the benevolence of the Web vendor,* which is about the consumer comprehension about the characteristics of the seller, such as caring, concern, good will etc. The authors mean that the way consumers are being handled and treated by the e-commerce's sellers, has a huge impact on the consumers trust towards e-commerce.

Belief in the integrity of the Web vendor is the second trusting beliefs factor, which is about qualities like honesty, carefulness, reliability, integrity and dependability. The authors mean that belief in integrity has a very significant role in order to gain trust. The category this belief belongs to is about, more or less, the consumers' privacy and their information, the privacy factors and personal information of consumers that the vendors have access to. According authors, it is very important to consider this belief of consumers very seriously, otherwise consumers would feel uncertain about sharing their privacy and personal information to the vendors, which results into mistrust being created among the consumers.

Further the third belief*, Belief in the competence of the Web vendor,* is about the product and service the vendors provide for the consumers. The authors claim that the service includes from the moment a consumer enters a Web site to the very end, which could

never gets end. Further they mean that very good service is required under the whole process (manufacturing, ordering, delivery, service after sale, solving consumers' problem and etc). The products' condition should be as good, if not better, as it is shown on the Web site, so the consumers do not feel tricked and get disappointed. The authors point out the importance of this belief and mean that the service giving to consumers, the way consumers experience the Web site and fulfilling of the consumers' expectations have an important role creating trust among the consumers.

The fourth and final trusting belief presented by the authors is *Belief in the predictability of the Web vendor.* This belief is based on two factors, predictability and consistency. The authors mean that an owner of a Web site should always try to reduce the potential risks, which provide mistrust among consumers. This category of belief aims to help consumers to determine *three consequences* of a vendor's trustworthiness. The first one is *consumer evaluation,* which is about the judgment of the consumers, if the vendor is trustful or not. The trust here determines if a transactional relationship, between the consumer and the vendor is being made or not. If the relationship is made, then the consumer will be willing to share his/her personal information with the vendor. The second one is *intention to use a vendor's site,* no matter for what purpose a consumer enters a Web site, it counts as he/she is there to seek information or for doing some kind of commercial transactions. And the authors mean that it is very important for the Web sites to have a layout that wins the consumers trust. The third one is called *actual visits to a site,* which means that it is important to create trust among users so they have the intention to use a vendor's Web site. The more consumers visit a Web site, the more Internet-based relationship gets exchanged, between the vendors and the consumers.

3.4.2 Seven critical factors that affect trust

The seven critical factors, presented by Ofuonye et al. (2008), which have huge effects on consumers towards companies or vice versa. The first one is *usefulness* which explains that the more a Web site is useful, the more it is trustful for the consumers. The authors mean that when a user gets involve with a Web site, she/he wants to achieve his/her goals in the simplest way. That is why a Web site should be very relevant for its users' goals. The second is *ease to use;* the easier it is to use a Web site, the more it contributes trust among consumers. The authors mean that it should not be hard for consumers to use the Web site and it should be easy for consumers to use the Web site in many ways. For example it should be easy to find the products they want to buy, to have access and find easily the information they need and etc. If a Web site misleads the consumers it results into mistrust among the consumers.

The third critical factor that affects trust is called *benevolence* and covers factors, which determines if the Web site acts in way that matches the users' best interests. The authors give a good example of this factor that is the trustworthiness of the information that is on the Web site. The authors mean that it is important that the information on the Web site is fully true and is not unbiased statements; otherwise the Web site could lose credibility among its consumers.

Competence is the forth factor, which describes the more competence the Web site's owner have, the more professional Web site becomes. The authors mean that professional functions and looks for a Web site are very important, since the factor professionalism has a significant role in creating trust among consumers. They also mean that things like errors and extensive use of animations give a feeling of lack of professionalism, which decrease the trust among consumers**.**

The fifth critical factor that affects trust wining e-commerce is *integrity,* which is a very sensitive and important factor regarding the consumers and that is why the authors mean that this factor should be considered very seriously by vendors. It should be clear for the consumers that the site considers the importance of honesty and ethical behavior, and consumers should not be concern about their privacy, personal information and identity. The authors also mean that the information given by consumers should not be misused by vendors in any way, in order to create and maintain trust among consumers. *Risk* is the sixth critical factor that should be oblivious for almost everyone. Everyone wants to be secure while doing businesses of any kind. When it comes to e-commerce, the willing of risks taking gets almost zero. According authors, the more risky to use a Web site is, the more it decreases the trust among consumers. The last critical factor is called *reputation*, which is about the views of people about the Web site. People could express their selves in different ways, for example by discussion boards on Web sites or their feedback given for the Web sites. The authors mean that the experience they have from a Web site could be both negative and positive. It affects a lot the reputation of the vendors, and it could affect the trust among the consumers both positively or negatively.

3.4.3 Secure trading for companies creates trust

According Tryggehandel.se, every company needs to create a good relationship with its customers in order to have a successful business. This success cannot be possible without creating a good trust between the companies and consumers. It is up to the companies to prove that every consumer should feel secured and have the trust from the company. In order to fulfill the demands and achieve success, twelve factors should be considered, which are mentioned bellow:

- Company's Detail

  The company's name and legal entity should be clearly stated. The visibility of registration number of the company, street address, e-mail address and phone number is vital. It makes it easy for consumers to find every needed details easily, in the time of complains or any other case. If there is any special opening hours for customers' support, times should be shown clearly on the site.

- The Company's Support and Availability

  The company should answer to customers question via e-mail within 48 hours from the minute they get it. If it is not possible in 2 days period, company should explain the reason of delay answer in order to have a good support and availability system. Company should show interests and give the costumers feeling of importance.

- The Consumer's Right to Get Help

  The consumer has always right to ask directly to the company for help with criticism, extraction and other assistance related to the purchase or order even if the company itself does not offer the product or service.

- Product and Total cost

  The consumers should assure that the product can be used in Sweden. The price of each product should be clearly written and all different costs like taxes, shipping cost and so on should be clarified. Product or service characteristics should be adequately described and available prior to a purchase agreement entered into between the buyer and seller.

- Delivery Time

  The consumer must be informed at time of purchase for maximum delivery time just after the order has been made. If the company cannot deliver the goods or services within the agreed time, the consumer should be informed as soon as possible. If it happens twice, the consumers have the right to cancel the purchase at no cost.

- Refunding

  The consumer has the right to recover the money within 30 days if he/she cancels an order from the date the company received the message.

- Return Policy

  The consumer should be informed and aware of withdrawal policy. The name and addresses where consumers can turn to, should also be elucidated. A consumer should have the right to return an already opened package to verify if the product works. With purchasing services, the service should be useful from the minute the agreement takes place. If service has been begun before the extraction period (14 days) expires, the company, with the consumer's approval, inform the consumer that the right of withdrawal ceases from the time service begins.

- Complaints and Seller's Guarantee

  The consumer must be informed of that existing at the complaints and the name and address where consumers can turn to. The consumer must be compensated for any shipping charges. Secure e-Commerce approved companies to promise to follow the Consumer Complaints Board's recommendations. The terms of any guarantees provided by the company must be disclosed. The consumer has the right to complain about a product or service if the product or service characteristics deviate from the agreed or provided by law.

- Manuals

  A product shall be alongside with the instructions in physical or digital form that the consumer need for use of the product, normally the instructions should be in Swedish.

- Sales to underage

  The company shouldn't have any business contract with underage (under 18) without the permission of parents or someone responsible.

- Financial Security

  The company must submit financial stability and good credit standing. It will be controlled regularly by an independent side.

- Secure Payment's Solution

  If the company itself or some other party have responsibilities for card data or other information in the time of direct transmission, they need fulfils the requirements for PCI DSS. It is the company's responsibility to develop a technology that enables the identification of the cardholders. With the saving of personal data of consumers by some company, the company is responsible to have permission from users. These personal data must be protected from any extern intrusion and should handle according to PUL.

3.5 Solutions for Security

As it already is mentioned in this study, security issues within e-commerce could be handled in many ways. Turban et al. (2010) claim that technology is one of those ways, maybe the most important way for solving the security issues within e-commerce. The authors present four phases in order to prevent or reduce security risks within e-commerce, which are explained briefly bellow:

- *Assessment*

  The authors mean that every kind of organization that is involved with the e-commerce, must always put a serious focus on their assets and make sure that they have a very secure security system, which protects their assets in the best way. Not only this but they should also know what the weaknesses of their system are and what factors could be threatening for these weaknesses? The authors mean that there are many ways to handle such problems, and one of the ways is to have an experienced and competent group of IT personal within the organization.

- *Planning*

  Planning could be a conclusive factor because nothing could be done right without planning. Turban et al. (2010) mean that every process, from the very simple issue to the very complicated one, needs a very good planning. The authors mean that the main purpose of this phase is to analyse which security threats the e-commerce companies might face, and what will be the costs to deal with these security threats? Further the authors claim that this phase should make it clear for the company which security threats are the most harmful and which threats should be prioritized, considering the possible damages caused by the threats and the costs to prevent them.

- *Implementation*

    When an organization is done with the planning phase, then it should put a good effort to determine what ways and technologies are the best to handle with these potential threats. According the authors, the first step in the phase implementation should be to choose common types of technologies for the high priority threats, and when this task is done then the specific software to deal with these threats should be chosen.

- *Monitoring*

    After going through those three phases mentioned above, then a company must continue with the phase monitoring, which never ends. The purpose of this phase is to evaluate which technology has been best to deal with security threats. What ways have been respectively successful and unsuccessful? What are the good and bad sites of the technologies being used, and what could be changed if necessary? Are there some new security threats that could befall the organization? Further the authors mean that the monitoring phase should give an acceptable answer for all these and other similar questions and this process should always be run periodic

Turban et al. (2010) moreover mention the importance of information being transited back and forward within e-commerce. They authors mean that information must always be fully protected by, among others, using best possible technologies. The information security system an organization using, must clarify that the legal parties to a transaction are totally identified, and the actions being done by the parties are lawfully allowed. Further, the system should not allow the parties to be able to do more tasks than needed, in order to fulfill the transaction. The authors also mean that an authentication system is a very useful system to achieve a good secured information system. The authors divide authentication system into five key elements.

The first element is *whether it is a person or a group*, both must be authenticated, and the second element is *both, a person or a group* where they must be differentiated from others, for example by something unique, a signature. *A very responsible administrator* is another element who should fully have awareness about the system's usage. The next element presented by the authors is *an authentication system or device*, which makes aware the organization about the attendance of the differentiating characteristic. Finally the last element is *the use of an access control mechanism,* which has the purpose to limit the actions being done by the authenticated groups or persons.

4. The result of empirical study

This chapter begins with a short presentation of the respondents and the four interviewed companies. Further, this chapter presents the result of the study's survey, which contains answers to interview questions.

4.1 The presentation of respondents and companies

Respondents:

- Respondent A: CEO (chief executive officer) and owner of company, with the 5 years of experience within e-commerce, 3 years within the company.

- Respondent B: Chief executive officer and owner of the company, with many years of experience as IT supplier and as well as within e-commerce.

- Respondent C: Supporter and adviser at the company. He Works, among others, with the technical solutions with the system of the Web shops made by the company.

- Respondent D: Chief executive officer of the company.

Companies:

Company A

This company is a Web shop that offers its customers children's clothes and accessories for the adults. What makes this company unique within the clothing branch is the fact that all products being offered are in Swedish folklore style. The three main factors, which play an important role in designs of the products being offered by this company, are inspiration from the Dalecarlia's folk costumes, the 19th-century design and Swedish rustic.

Company A is very big and well known in the Dalecarlia, since the design of products, offered by the company, got its basis from Dalerclia, where the manufacturing of the products take place as well.

Company B

The brand of this company was created in the beginning of 1990s in Gothenburg, Sweden. The target group of this company was children and mostly had cloths for children. Company B decided to make an effort to expand the business further in Sweden. During several years of success in the 90s and start of 20s, the children's cloth branch improved largely, which resulted with an increasing of approximately 30 more stores, throughout Sweden from Luleå in the north to the south. During the late 2000s terminated the company's physical stores.

After finishing with the company's physical stores, the new online era started with same brand name. Today, the personals and sellers who work for the company has more than 15 years work experience at company's physical stores who still work in this new format, Web shop. The Web shop aims to offer its customers a good variety of fashionable children's clothing at the right price with a level of customer service beyond customer expectations.

Company C

Company C helps its consumers with getting start whit Web shops. This company develops wanted Web shops for its consumers and rent it for monthly pay. The company was created in the autumn of 2000, which gives the company an experience of more than 10 years in the e-commerce's field. The founder of the company still is the CEO and owner of the company. The company got its base in Malmö, Sweden.

Company D

Company D is an innovative Web agency, which is specialized within e-commerce. It was established in 2005 and it is one of the Sweden's leading suppliers of e-commerce. This Company provides an e-commerce's system of its own for its consumers. The idea is to offer products and service for the consumers who wants to start and develop business on the Internet.

4.2 Interviews

Security and trust within e-commerce

Two of the companies claim that security within e-commerce is a vital factor to be considered and means that security factors should be faced very seriously. They also indicate that both of the companies are very good at dealing with the security questions. When it comes to Web shops, they are very dependable on their system's supplier, according them. They mean that their system supplier stands for the security of their system, which means that both Web shops do not have a complete control on their Web shop system. Regarding security demands on company, both from the company its self and from consumers, one of the Web shops claims that no security demands have been made from the company's consumers, but on the other hand the company has some clear security demands, which are to have a trustworthy plus secure e-commerce system and to be competitive. Supporter and adviser of one of the companies prioritizes the importance of having demands on security very high, and points out the renewing of their system that is more secure. On the other hand, the owner of one of the companies states that no security demands are required nor needed from any party.

According to one of the respondents, to have a secure e-commerce company, three main factors should be seriously considered, namely sensitive information, personal information and payment methods. He means that these three factors should be handled in the most secure way. However, another respondent does not have the same thinking about the importance of these three factors, and means that it would not be a big loss if

something goes wrong whit any of those three factors. On the other hand, another respondent who has the CEO position means that besides having a secure technology, the design, layout, professionalism of a Web shop give a trustworthy and secure feeling to the consumers.

"Secure e-commerce is that consumers' sensitive information, personal information and payment information should be stored in a trustworthy way, not only stored but also handled in a trustworthy way." (Supporter and adviser of company C)

The Problems of Security and Trust

Two of the companies never have experienced any kind of security problem, according to the respondents. CEO and owner of one of the companies mentions about the internal security problem they have had. He refers to the problems with their programming that went wrong and caused some security issues. Further he explains that the problem was solved by reprogramming the system, and means that e-commerce system should always be updated to face new security issues.

CEO of another company on the other hand believes that the security problems within e-commerce have dramatically decreased from before. He assumes that problems caused by bank payments within e-commerce are not that common as they were. He further names other problems, like crushing of hard drives, which could create serious security problems for an e-commerce company. Even another CEO of a Web shop mentions the problems her company had when they replaced their platform to a new one. She means that the new system itself was a better one from the previous, but during the changing process there were disorders in the system. For example when at the time of confirming a purchase weird characters were shown up on the screen, which created security instability for both, the company and consumers.

An owner of interviewed companies points out a very broader security problem within e-commerce, which is the bad influence of world's mafia on e-commerce's security. He means that mafia hacks the e-commerce's systems and causes very serious problems. Another respondent on the other hand, points out the usual and daily problems within e-commerce. He means that security problems will always be there, due to the continually development of the e-commerce's system. He also points out a security problem that occurs often, which is the misusing/stealing of the bankcard's account information, while consumer filling needed information during an online purchase.

According CEO and owner of one company, the level of trust differs from generation to generation within e-commerce, which is why he wishes that the trust within e-commerce should get better among all ages. Another problem that creates big trust issues is the lack of the sources in some Web shops, according to technique supporter and adviser at one of the Web shop system's supplier. He further claims that such Web shops, which have just sources of their own, could be fake and trick consumers.

The solutions of Security and Trust

CEO at the one Web shop means that having serious focus on the question about the security within e-commerce, is a must factor in order to solves security issues. Obvious and useful security demands should be implemented on e-commerce's companies. She also means that suggestions/complaints about the security issues, from both parties, should be listened and debated seriously. Further she points out the important role banks playing in order to maintain a secure e-commerce system. For example banks should require more than just bankcards while consumers purchase online, maybe a special code or payment box along whit the bankcard. She also mentions the importance of passing some kind of security test before a Web shop get permission to start the business. Another respondent also agrees whit the security test, and recommends the association Trygg E-handel(Secure E-commerce). He means that to get a certificate from Trygg E-handel and have their logo on the Web site means that the Web shop's system is highly secured. He even points out the important role of authorities and increasing of e-commerce's suppliers.

"As e-commerce is growing a lot, then surely, increase the interests and so do the suppliers of security and even authorities. There is focus because there is money. As long the e-commerce grows, the security will exist and get better." (CEO of company B)

To have a good understanding of the security level, one of the companies regularly running different kind of security testes, claims the company's CEO. Even the technique supporter of another company thinks that security testes are an important way of dealing with the security issues, and claims that the their system's developers run security testes in order to identify the possible security risks in the system. He claims that testes are run as often as it is needed, and when new functions are established in their system then new sorts of testes are being done. One of the Web shops does some kind of survey about the consumers' satisfaction level, and Web shop's owner refers the satisfaction of consumers to the security factor. The other Web shop on the other hand, does not perform any kind of security test at the moment, but according the company's CEO they will, in the near future, begin with some kind of security test.

Another respondent who owns the company and has a position as CEO means that a company should secure both, internal and external, sources. For example by encrypting the company's hard drives and making aware the consumers about how they can be secured online, like having a proper password and etc. another respondent on the other hand, brings up the importance of changing the system when it is needed. He gives an example of the new system they recently have launched. According him the new system has a higher security and it has many advantages, for example, it sorts the whole traffic taking place in the system and the entire transaction takes place in the highest security level. Further another respondent also believes on changes for the better. She means if a current way/factor does not function proper and secure, then it should be changed for good. She backs up her statement by giving an example of changing for better they have done, namely the change of their platform. She means that things began to work in a better way when the platform was changed.

"The absolute best thing is that we show that we really exist; we have a clear organization with clear contact information, e-mail addresses, showing photos of our staff, are good at explaining the products and provide all needed information. This creates incredible good trust among customers." (CEO of company D)

One of the CEOs brings up the significance of having the trust of consumers within e-commerce, and claims that every company should try to reduce the trust issues among the consumers. He means that the trust of consumers could be gained by showing/proving to consumers that the Web shop is real and not fake. Further he claims that they are very good at solving this trust problem, by having a legible organization with a clear contact information, e-mail addresses and pictures of the employees. Further he adds that the company should describe the products in a very good way. He also says that the company should make all the needed information available about the products for the consumers, which leads to gain the consumers' trust in a best possible way. One of the CEO's solutions for reducing trust issues matches almost totally the other respondents' ideas for gaining consumers' trust. She means that consumers are not that canny when it comes to technology, they believe at what they see, which is conclusive for gaining the consumers trust. Two other factors, good communication with the consumers and obvious payment methods, solve the trust issues among the consumers, according two other respondents.

"Our consumers are not good at technology. Which e-commerce suppliers are good do not know our consumers, their trust is based on their experience of the Web shop, so it is the experience of the consumers that creates/destroys the trust among them for the e-commerce." (CEO of company A)

4.3 Payment method's pros and cons, and its affect on trust

One of the Web shops offers its consumers three payment methods that are card payment, invoice and COD (Cash On Delivery), and according the company's CEO every method has its pros and cons, from the security point of view. According her, the bankcard payment is the securest method for the companies and for the consumers the invoice is the securest, out of those payment methods her company offers. She means that with the bankcard payment method an e-commerce company always get paid before delivering the products, if there is not any money in the bank account the delivery will not take place. And the reason why invoice is securest for the consumers is the fact that consumers do not need to give out their bankcard's information, and she says in addition that COD method ends up at last for both parties. However, another respondent affirms that both card payment and invoice (the only two payment methods the company has) are equally trustworthy and secure for company, because the company will get its payment guaranteed with either method. But, he adds, for the consumers the method invoice could be the securest, considering the sensitivity of bankcard's details and the fact that consumers get the products earlier than with the card method. He also means that COD method gets the third place, after bankcard and invoice, for the companies, and second place for the consumers.

According one of companies' technique supporter and adviser, every payment method is secured for a company and means that the company gets its payment anyways whit any method. According him, they offer many different payment methods as card payments, invoice, COD, direct payment through banks and etc. He means that, out of all payment methods, invoice could be the securest for the consumers, following by COD and bankcard methods, because consumers get the chance to receive the products before paying for the products. On the other hand, CEO at one of the companies claims that the card payment method is the securest method for the consumers, following by COD and invoice, since consumers get back their money from the bank if something goes wrong. He evaluates card payment as an unsecure method for the companies, regarding the fact that if someone misuses someone else's bankcard and purchases something with it online, then the company will not get any compensation for the delivered products but the owner of the card will get his/her money back from the bank. He also means that invoice comes at the first place and COD at the third, from security point of view for the companies.

CEO at one of the Web shops is satisfied with the three current payment methods they offer. She motivates her satisfaction by feeling secured with the company's current payment methods, and claims that it feels a bit unsecure with the other payment methods, like Paypal and others. She and another respondent mean that the payment methods they offer are the most demanding and common at the moment. Further, she claims that the current security for the payment methods within e-commerce is much secured, and to even make it better every company should put good effort on the layout of the Web shop. Another CEO also thinks the payment security is good enough and off course, like every other thing, it could get better and better. He also mentions that the e-payment's security is better for the consumers than companies, due to the loss of money for the company if someone uses a stolen bankcard in order to purchase online.

Level of security from 1 to 3	Company A	Company B	Company C	Company D
1	Bankcard & Invoice	Bankcard	Any payment method	Invoice
2		Invoice		Bankcard
3	COD	COD		COD

The level of security for different e-payment methods for companies, according the interviewed companies

Further one of the owners explains the importance of not getting a victim of payment frauds, as a company. She means if such an incident takes place the company will lose its credibility among its consumers. She means that it takes just a consumer blogging

somewhere about the incident and many other will lose the trust for the company, no matter if it's the company's fault or the company's suppliers'. She includes the importance of preventing such incidents and means that a company should use the securest available technology. Further she adds, if such incidents take places the company must have good and reliable insurance companies as its supplier, so the consumers get paid for the damage caused.

Level of security from 1 to 3	Company A	Company B	Company C	Company D
1	Invoice	Invoice	Invoice	Bankcard
2	COD	Bankcard	COD	COD
3	Bankcard	COD	Bankcard	Invoice

The level of security for different e-payment methods for consumers, according the interviewed companies

Regarding future, one of the respondents believes that other payment methods going to be more popular than the methods that are mostly used today. According her, methods like Paypal and other direct payment methods from bank going to be more popular than methods like card payment and invoice. But at same time, she means that those methods should feel secured, both for the companies and consumers, in order to gain the top popularity.

Company	Most popular e-payment method in 5-10 years
A	Bankcard
B	Direct payment methods from Banks
C	Invoice
D	Other new methods that require identification of the user

Most popular e-payment method, according interviewed companies

On the other hand, another respondent believes in the establishing of new payment methods in the future. He means that some kind of personal payment system will be created, a system that requires consumer's identity in order to purchase online. The

payment would be stored personally at the consumer's, not at his card's account or through invoice. On the other hand another respondent who has a position as technical supporter believes that the payment method invoice will rule in the future. However, one of the Web shop's CEO believes that bankcard method will be the most popular, because in 5-10 years the generation will be more familiar with e-commerce and their trust for e-commerce will be better.

5. Discussion

This chapter is an analyzes based on information that study obtained from the empirical framework in the form of interviews with respondents and literature study which is presented in chapter three of this study. This analyze discusses the general facts, problems and solutions that is gathered about security and trust within e-commerce

By going through the literature study and empirical study, we think there are some lacks regarding security and trust within e-commerce. We also think that the e-payment methods that are being offered are not totally good enough, and the reason is that we got different responds from the interviewed companies regarding the most secure e-payment method. If an e-payment method is not the most secure according the all four companies, in that case there must be something not good enough about the method.

From our literature study we have understood that technology plays an important role in the security of e-commerce, and to have staff that are good at technology is something every company should consider. Further, from our empirical study we got to know that not every company have the staff who are enough knowledgeable about the technology regarding e-commerce. Such companies are very reliable on their suppliers, which is not that good according us. We think that having at least one person, who is very good at technology, within the company, is almost a must factor in order to handle security issues in the best way.

On the other hand, both literature and empirical studies showed that consumers trust could be gained mostly by have a professional layout on the Web site. We got to know that consumers' experience affects their trust. Sensitive and personal information should be highly prioritized according the literature study, which we totally agree with. The importance of these two factors was mentioned in the empirical study as well, though not by all of the interviewed companies. It was very surprising for us that one of the companies did not think it would be a big deal if something goes wrong whit the consumers' sensitive and personal information.

A very good point has been noticed by us in the theoretical part, which is the fact that many companies view the security often as an IT problem and not organizational. This mistake was shown in the empirical study as well. Two of the companies would not feel responsible within organization if something would go wrong with their IT factors. They would turn their selves for the external help, which is their supplier. The literature study brings up the importance of updating or changing the system when it is needed, and to update the knowledge and skills of the company's staff. In our empirical study we have seen some of these challenges. Some of the companies claimed that they have changed their system to meet the security challenges in the best way, while others were satisfied whit the current system. However, we think none of the interviewed companies were good at updating of staff's knowledge or skills, and their reason was that it was not needed.

According the literature study many ordinary people try to break into the Web server of the companies and cause different kind of security issues. From the literature study we have got an understanding that it is not very unusual that people try to damage companies' system and cause security issues. Interestingly, we didn't get really the same understanding from our empirical study. The companies have never had such problems, and they mean that their system is so secured that it is almost impossible for the outside users to do something wrong with our system. With all due respect to the companies, we don't think that is true. In today's age, the biggest companies could be victim for such acts.

One of the solutions, given in literature study part, for handling the trust issue among consumers, companies should be very good at providing the needed information about the products and good service. The service includes the moment a consumer enters the Web site to the very end. This factor was brought up in the empirical study as well. Almost all the interviewed companies claimed that they are very generous when it comes to servicing the consumers under the whole process. This is a factor which we think is very important every e-commerce's company should take seriously. Another factor which is mentioned in both, literature and empirical study is that the Web site should give the consumers an expression of being real, i.e. the Web site should not be felt as a fake one when consumers use it.

From our empirical study we have come up with the fact that two types of e-payment methods are the most common and secure within e-commerce, namely bankcard payment and invoice. The interviewed companies would rank, from the security perspective, these two methods a bit differently. But to sum it up it could be said that the interviewed companies think the bankcard method is the securest for the companies and the invoice is the securest for the consumers. We have to agree at this point with the companies, since giving out the bankcard's information on the Web sites does not seem a very secure option for the consumers. On the other hand, for the method invoice not much important information is need to be given out.

6. Conclusion and future researches

This chapter presents the conclusions that have been obtained from this study. In addition, the chapter also includes the recommendations that are considered essential for further studies on subject of this study.

- **Which factors create common security issues within e-commerce?**

The study shows that there are many factors that create security issues within e-commerce. One of the factors that causes security issues is the fact that many companies focus just on securing their internal networks and fail to understand the security practise of their supply chain partners. The study also shows the carelessness of some companies about focusing on security before something goes wrong, i.e. most companies focus on security after an incident or problem occurs. Another factor that causes serious security issues is to not updating or changing the companies' security practices in order to meet changing needs. Viewing the security issues as only an IT problem but not organizational issue is another important factor which causes security issues, within many companies. Further the study points out one of the very important factors that creates security issues within e-commerce, which is bad technology. One does not need to be a supper hacker in order to break into a Web server of the companies and cause different kind of security issues, if he/she is facing a bad technology. This study also proves the lack of IT competence within some Web shops, which makes them vulnerable regarding security risks

- **Which factors create mistrust among the consumers of e-commerce?**

One of the most common factors that creates mistrust among the consumers is the question of reality of the Web site, i.e. if the Web site is totally legitimate and legal. The study shows that fake Web sites are being made in order to trick consumers, which dramatically affect negatively consumers' trust. Even if the Web site is legitimate and legal, it still could damage the consumers trust by not convincing the consumers. That is why unprofessional look of the Web sites is very decisive factor on creating mistrust among the consumers. Further the study shows another factor that creates mistrust among the consumers, which is the misuse of the consumers' personal and sensitive information. The misuse could be done in many ways, for example if the information is used for the wrong purpose or if someone unauthorized get access to it. The study also shows that fraud done within different e-payment methods creates very serious trust issues among the consumers.

- **Which solution can be used to prevent/reduce security issues within e-commerce and how to create trust among the consumers?**

This study shows clearly that technology plays a conclusive role in building of security and trust within e-commerce. The interviewed companies claim they have the technologies that make it impossible for taking place of security risks, which is very doubtful. If such technologies were in use, why so much security risks would exist within e-commerce? Not just having good technologies is important for a secure e-commerce, but also skilled staffs are required in order to understand and develop these technologies. Further the study proves that secured e-commerce could be gained by a better role of banks that could be played, when it comes to e-payment methods. Security testes are another solution that could contribute a lot for improvement of the e-commerce's security. Every company that get starts business within e-commerce should go through some kind of security test.

The study describes the importance of updating of the system or maybe changing all the system if it is needed in order to solve the security issues within e-commerce. Further the study brings up the very important role of training the staffs to update their knowledge in order to face the new security issues within e-commerce. Another solution that is shown by this study is to have good planning and to know which security issues should be prioritized first. Some security issues can be very damaging and some of them can be less damaging, and a company should know which security issues should be handled first in order to secure the company's system.

This study also shows that the consumers' experience is very important in order to trust a Web shop. How a user experiences a Web shop could be decisive for his/her trust towards the Web shops. This study substantiates that some Web shops put lots of effort rather, on making better the consumers' experience of a Web site, than on the technological factors. In order to have a trustworthy Web site; it is vital to have a professional design and layout on the website. Further, the study argues that the visibility of the Web site plays a significant role to improve trust among consumers. Factors that can contribute to a better visibility could be the logo, company's legitimate, postal address, e-mails address and contact numbers, which should be clearly shown on the Web site.

Study explains that a good service and valuable treatment increase consumers' level of trust. It is important that the consumers do not feel tricked in order to gain their trust. Real, detailed and valid information on Website is vital in order to increase trust. The study explains that consumers are very careful when they share their personal and sensitive information and in order to convince them to trust the Web site, the companies should create a good relationship with consumers. This relationship can be created by communication and good service. The study also recommends the companies to use the authentication system, which is very useful system in order to achieve a good secured information system

Going through this study, it can be cleared that it is almost impossible to get rid of all the trust and security issues within e-commerce. The issues will always be there, due to the continually development of the e-commerce's system. The development its self creates complexity that brings up issues. But, if right methods are used, the issues could be reduced. From the study it could also be understood that different e-payment methods that are being offered are not totally good enough, and the reason is that different responds were received from the interviewed companies regarding the most secure e-payment method. If an e-payment method is not the most secured according to the all four companies, then there must be something not good enough about the method.

Further researches

The fact that e-commerce is a branch that is being developed very vastly, makes it more and more interesting for the people within different business. At the same time the use of e-commerce is becoming more and more common among the users. Therefore, useful researcher should be done to find ways/technologies to meet the development of the e-commerce at the best ways. The most important factors are security and trust within e-commerce, which is why researches should be taking place, in order to make the security and trust issues vanish totally within e-commerce. Further researches should contribute to consumers feeling as trustworthy and secure doing businesses online, as they feel doing businesses offline. Methods should be created that gain totally consumers' trust towards companies.

Another interesting area within e-commerce is international e-market. Researches about the consumers from other countries would be useful, for example how to gain their trust and how difficult it is, compared with the local consumers. Researches on different e-payment methods should also be done. Better and securer e-payment methods should be created in order to make online purchases as normal and secure as offline.

7. References

Moores, T. T. & Dhillon, G. (2003) *Do privacy seals in e-commerce really work?* Communications of the ACM Vol. 46, No. 12 December 2003, p. 265-271

Carr, D. L. et al. (2010) *The impact of instructor attire on college student satisfaction,* Collage Student Journal Vol. 44 , No. 1 March 2010, p. 101-111

Salam, A.F. et al. (2005) *Trust in E-commerce,* Communications Of the ACM Vol. 48. No. 2 February 2005, p. 73-77

Ejike, O. et al. (2008) *How do we build trust into e-commerce Web sites?* IEEE SOFTWARE, September/October 2008, p. 7-9

Rusch, J.J. (2003) *Computer and Internet Fraud: A Risk Identification Overview,* US Department of Justice Vol. 2003. No. 6 June 2003, p. 6-9

Erfaim, Turban. et al. (2010) *Electronic Commerce: A managerial perspective*, Pearson Education LTD

Padhyay, B. N. (2002) *E-commerce: context, concepts and consequences,* McGraw – Hill International (UK) Limited

Dykert, L. et al. (2002). *E-business- för tillväxt och lönsamhet*. Lund: Studentlitteratur.

Alan, B & Emma, B. (2005). *Företagsekonomiska forskningsmetoder.* Malmö: Liber ekonomi.

Dykert, L & Ange L. (1997). *Elektroniska affärer juridisk och revision.* Lund: Studentlitteratur.

Prins, J.E.J. et al. (2002). *Trust in Electronic Commerce- The role of Trust from a Legal, an Organizational an a Technical Point of View.*

Jack, H. (2005). *100 sidor om att starta, driva och marknadsföra en butik på Internet.*

www.tryggehandel.se/?sida=krav
www.guppi.se
www.emylittle.se
www.startabutik.se
www.starweb.se

8. Appendix

Intervju frågor till C-uppsatsen inom E-handel, mer riktad på Säkerhet och tillit inom E-handel.

Uppsats undersökaren:

Anil Haidari
Khushal Paktiani
IT universitet, Göteborgs universitet,

Företagande

Bakgrundsinformation

◦ Namn _____
◦ Företag _____
◦ Befattning _____
◦ Bransch _____
◦ Antal års erfarenheter av E-handel ____ år

En kort beskrivning av det Er verksamhet gör:

Säkerhet inom E-handel

1) Beskrivning av hur er verksamhet ser på faktorer nedan:

   - Säkerhet

   - Personlig integritet

   - Känslig information

   - Tillit

2) Vilka åtgärder görs vid hanteringen av ovanstående tre faktorer?

   - Sätts det upp några krav för förbättringen av dessa tre faktorer?

      • I så fall från vilka sätts upp dessa krav? Er? Kunder? Eller både?

         - Vilka typer av krav sätts i så fall?

         - När sätts upp dessa krav? Förre eller efter risker för dessa tre faktorer?

3) Hur är en säker E-handels verksamhet enligt Er?

4) Vilka faktorer är viktigaste att en säker e-handel ska nås? Gärna motivera

5) Gör ni något för att kolla Er e-verksamhets säkerhets grad?

   I så fall:
       Hur ofta?

       När?
   - Under eller efter utvecklingen?

6) Har Ni blivit utsatta för någon/några typ av säkerhetsproblem? Vilket/vilka?

- I så fall hur har ni hanterat det?

- Kunde det hanteras på ett bättre sätt idag?

7) Har Ni någon/några allmän säkerhetspolicy för er verksamhet?

- Om ja:

- Hur bidrar det till lösandet av säkerhetsproblemen?

- Vilka sorts av säkerhets problem lösas och vilka inte med er säkerhetspolicy?

8) Vad blir det för konsekvenser om säkerhetspolicyn inte följas (både för e-handels organisationer och dess kunder)?

- Hur påverkas både er verksamhet och konsumenterna?

9) Tidigare säkerhets hot inom e-handel (både för e-handels organisationer och dess kunder)?

- Finns de fortfarande kvar? Varför?

- Om inte, hur har man lyckats med det?

10) Säkerhets hot som finns idag inom E-handel (både för e-handels organisationer och dess kunder)?

- Varför finns dessa?

11) Brukar det finnas behov av utbildningar, för personal i er verksamhet, som går ut på e-handels säkerhet? I så fall hur ofta?

12) Tror ni det läggs tillräcklig fokus på säkerhets faktorer inom E-handel i dagens läge? Motivera gärna.

Tillit inom E-handel

1) Vilka faktorer påverkar mest tilliten, hos kunder och företagande, inom E-handel?

- Positivt, motivera.

- Negativt, motivera.

2) Vad har ni för förtroende till er kunder? Bra/dålig, varför?

3) Hur bra/dålig är era kunders förtroende till Er? Varför?

4) Hur upplever Ni tilliten inom E-handel i nuläget?

- Tillräckig bra? Varför?

- Kan förbättras? Hur?

5) Hur kan tillit inom e-handel förbättras?

Betalningsätt inom E-handel:

1) Vilka betalningssätt erbjuder Ni till era kunder?

- Vilka av dessa är säkraste och osäkraste(för Er och kunderna)? Rangordna gärna och motivera varför.

2) Vilka betalningssätt erbjuder Ni inte? Varför?

3) Vad har ni för åsikter om betalningssäkerhet som erbjuds inom e-handel? Bra/dålig? Varför?

4) Vad tycker Ni just om Er betalningssäkerhet?

- Kan förbättras? I så fall hur?

5) Har Ni/Er kunder blivit utsatta för bedrägeri vid elektroniska betalningssätten?

Om ja:
- Hur ofta händer det?

- I vilka grad påverkar det kundernas tillit för E-handel?

- Hur kan man hindra/minska det och öka kundernas förtroende?

6) Saknar Sverige något/några säkrare betalningssätt inom E-handel? Motivera.

7) Vilket/vilka betalningssätt är populära inom dagens E-handel ur säkerhets perspektiv?

8) Vilka betalningssätt tycker Ni kommer vara populära i framtiden (om 5-10 år) ur säkerhets perspektiv? varför?

Önskar ni att Ert företags namn ska publiceras i vår akademiska uppsats eller vill Ni vara anonym?